Edge-corE

Powered by Accton

ES4704BD
4 Slots L2/L3/L4 Chassis Switch

User's Guide

www.edge-core.com

Preface

ES4704BD is a high performance routing switch released by Edge-Core that can be deployed as the core layer device for campus and enterprise networks, or as an aggregation device for IP metropolitan area networks (MAN). ES4704BD provides 4 slots, with support for various types of line cards and can seamlessly support a variety of network interfaces from 100Mb, 1000Mb to 10Gb Ethernet.

We are providing this manual for your better understanding, use and maintenance of the ES4704BD. We strongly recommend you to read through this manual carefully before installation and configuration to avoid possible malfunction or damage to the switch. Furthermore, we sincerely hope our products and services satisfy you.

Content

CHAPTER 1 PRODUCT OVERVIEW 32

1.1 PRODUCT BRIEF 32

1.1.1 Introduction 32

1.1.2 Features 32

1.1.3 Main Features 35

1.2 TECHNICAL SPECIFICATIONS 35

1.3 PHYSICAL SPECIFICATIONS 36

1.4 HARDWARE COMPONENTS 36

1.4.1 Chassis 37

1.4.1.1 Board Rack 38

1.4.1.2 Power Supply 39

1.4.1.3 Ventilation and Cooling System 39

1.4.2 Introduction to ES4704BD cards 39

1.4.2.1 EM4704BD-M12GX-SFP 39

1.4.2.1.1 Front Panel 40

1.4.2.1.2 Front Panel - Indicator 40

1.4.2.1.3 Front Panel Port Description 41

1.4.2.1.4 Front Panel – Console Port 41

1.4.2.1.5 Front Panel – Management Port 42

1.4.2.1.6 Front Panel – Reset Button 42

1.4.2.1.7 Front Panel – SWAP Button 42

1.4.2.2 EM4704BD-M24TX4GC 42

1.4.2.2.1 Front Panel 42

1.4.2.2.2 Front Panel - Indicator 43

1.4.2.2.3 Front Panel Port Description 44

1.4.2.2.4 Front Panel – Console Port 45

1.4.2.2.5 Front Panel – Management Port 45

1.4.2.2.6 Front Panel – Reset Button 45

1.4.2.2.7 Front Panel – SWAP Button 45

1.4.2.3 EM4700BD-12GT-RJ45 45

1.4.2.3.1 Front Panel 46

1.4.2.3.2 Front Panel - Indicator 46

1.4.2.3.3 Front Panel Port Description 46

1.4.2.3.4 Front Panel – Reset Button 47

1.4.2.3.5 Front Panel – SWAP Button 47

1.4.2.4 EM4700BD-12GX-SFP 47

1.4.2.4.1 Front Panel 47
1.4.2.4.2 Front Panel - Indicator 47
1.4.2.4.3 Front Panel Port Description 48
1.4.2.4.4 Front Panel – Reset Button 48
1.4.2.4.5 Front Panel – SWAP Button 49
1.4.2.5 EM4700BD-2XG-XENPAK 49
1.4.2.5.1 Front Panel 49
1.4.2.5.2 Front Panel - Indicator 49
1.4.2.5.3 Front Panel Port Description 50
1.4.2.5.4 Front Panel – Reset Button 50
1.4.2.5.5 Front Panel – SWAP Button 50
1.4.3 EM4704BD-AC 50
1.4.3.1 EM4704BD-AC (Alternating Current Power Module) 51
1.4.3.2 Power module Front Panel 51
1.4.3.3 LED 51
1.4.3.4 Switch of power supply for front panel 51
1.4.4 Power Distribution Box 52
1.4.5 System Backplane 52
1.4.6 Fan Tray 52
1.4.7 Dust Gauze 53
1.4.8 Rear Panel 54
1.4.9 Side Panels 54
1.5 SYSTEM FEATURES 55
CHAPTER 2 HARDWARE INSTALLATION 56
2.1 SAFETY INFORMATION 56
2.1.1 Site Requirements 57
2.1.2 Temperature and Humidity Requirements 57
2.1.3 Dust and Particles 58
2.1.4 Preventing Electrostatic Discharge Damage 59
2.1.5 Anti-interference Requirements 59
2.1.6 Rack Configuration 59
2.1.7 Power Supply Requirements 60
2.2 PREPARING FOR INSTALLATION 60
2.2.1 Checking Switch Hardware Configuration and Accessories 60
2.2.2 Required Tools and Utilities 61
2.3 HARDWARE INSTALLATION 61
2.3.1 Switch Installation 62
2.3.1.1 Desktop installation 62

2.3.1.2 Rack-mounting ES4704BD 62
2.3.1.3 Wearing an ESD Wrist Strap 63
2.3.2 Switch grounding *64*
2.3.3 Card and module installation *65*
2.3.3.1 Removing and Installing the Cards 65
2.3.3.2 Removing and installing the Dust Gauze 65
2.3.3.3 Removing and Installing the Fan Tray 66
2.3.3.4 Removing and Installing Power Supply Modules 67
2.3.4 Connecting to the console *67*
2.3.5 Connecting to the Management Port *68*
2.3.6 SFP transceiver installation *68*
2.3.7 XENPAK transceiver installation *68*
2.3.8 Copper Cable/Fiber Cable Connection *69*
2.3.9 Power supply connection *69*

CHAPTER 3 SETUP CONFIGURATION 71

3.1 SETUP CONFIGURATION 71
3.1.1 Main Setup Menu *71*
3.1.2 Setup Submenu *72*
3.1.2.1 Configuring switch hostname 72
3.1.2.2 Configuring Vlan1 Interface 72
3.1.2.3 Telnet Server Configuration 73
3.1.2.4 Configuring Web Server 75
3.1.2.5 Configuring SNMP 76
3.1.2.6 Exiting Setup Configuration Mode 78

CHAPTER 4 SWITCH MANAGEMENT 79

4.1 MANAGEMENT OPTIONS 79
4.1.1 Out-of-band Management *79*
4.1.2 In-band Management *83*
4.1.2.1 Management via Telnet 83
4.1.2.2 Managing the Switch through ECview 86
4.2 MANAGEMENT INTERFACE 86
4.2.1 CLI Interface *87*
4.2.1.1 Configuration Modes 87
4.2.1.1.1 User Mode 87
4.2.1.1.2 Admin Mode 88
4.2.1.1.3 Global Mode 88
4.2.1.1.3.1 Interface Mode 88

4.2.1.1.3.2 VLAN Mode 89
4.2.1.1.3.3 DHCP Address Pool Mode 89
4.2.1.1.3.4 Route Mode 89
4.2.1.1.3.5 ACL Mode 89
4.2.1.2 Configuration Syntax 90
4.2.1.3 Shortcut Key Support 90
4.2.1.4 Help function 91
4.2.1.5 Input verification 91
4.2.1.5.1 Returned Information: success 91
4.2.1.5.2 Returned Information: error 92
4.2.1.6 Fuzzy match support 92
4.3 WEB MANAGEMENT 92
4.3.1 Main Page 92
4.3.2 Module Front Panel 93
CHAPTER 5 BASIC SWITCH CONFIGURATION 94
5.1 BASIC SWITCH CONFIGURATION COMMANDS 94
5.1.1 clock set 94
5.1.2 config 94
5.1.3 enable 94
5.1.4 enable password 95
5.1.5 exec timeout 95
5.1.6 exit 96
5.1.7 help 96
5.1.8 ip host 96
5.1.9 hostname 97
5.1.10 reload 97
5.1.11 set default 97
5.1.12 setup 98
5.1.13 language 98
5.1.14 write 98
5.2 MAINTENANCE AND DEBUG COMMANDS 98
5.2.1 ping 98
5.2.2 Telnet 100
5.2.2.1 Introduction to Telnet 100
5.2.2.2 Telnet Task Sequence 100
5.2.2.3 Telnet Commands 101
5.2.2.3.1 monitor 101
5.2.2.3.2 telnet 101

5.2.2.3.3 telnet-server enable 102
5.2.2.3.4 telnet-server securityip 102
5.2.2.3.5 telnet-user 103
5.2.3 traceroute 103
5.2.4 show 103
5.2.4.1 show clock 103
5.2.4.2 show debugging 104
5.2.4.3 show flash 104
5.2.4.4 show history 104
5.2.4.5 show memory 105
5.2.4.6 show running-config 105
5.2.4.7 show startup-config 106
5.2.4.8 show switchport interface 106
5.2.4.9 show tcp 107
5.2.4.10 show udp 107
5.2.4.11 show telnet login 108
5.2.4.12 show telnet user 108
5.2.4.13 show version 108
5.2.5 debug 109
5.3 CONFIGURING SWITCH IP ADDRESSES 109
5.3.1 Configuring Switch IP Addresses Task Sequence 109
5.3.2 Commands for Configuring Switch IP Addresses 110
5.3.2.1 ip address 110
5.3.2.2 ip bootp-client enable 110
5.3.2.3 ip dhcp-client enable 111
5.4 CONFIGURING SNMP 111
5.4.1 Introduction to SNMP 111
5.4.2 Introduction to MIB 112
5.4.3 Introduction to RMON 113
5.4.4 Configuring SNMP 114
5.4.4.1 SNMP Configuration Task Sequence 114
5.4.4.2 SNMP Configuration Commands 115
5.4.4.2.1 rmon 115
5.4.4.2.2 snmp-server community 115
5.4.4.2.3 snmp-server enable 116
5.4.4.2.4 snmp-server enable traps 116
5.4.4.2.5 snmp-server host 117
5.4.4.2.6 snmp-server securityip 117

5.4.5 Typical SNMP Configuration Examples 118
5.4.6 SNMP Troubleshooting Help 119
5.4.6.1 Monitor and Debug Commands 119
5.4.6.1.1 show snmp 119
5.4.6.1.2 show snmp status 120
5.4.6.1.3 debug snmp packet 121
5.4.6.2 SNMP Troubleshooting Help 121
5.5 SWITCH UPGRADE 122
5.5.1 BootROM Upgrade 122
5.5.2 FTP/TFTP Upgrade 124
5.5.2.1 Introduction to FTP/TFTP 124
5.5.2.2 FTP/TFTP Configuration 126
5.5.2.2.1 FTP/TFTP Configuration Task Sequence 126
5.5.2.2.2 FTP/TFTP Configuration Commands 128
5.5.2.2.3 copy（FTP） 128
5.5.2.2.4 dir 129
5.5.2.2.5 ftp-server enable 129
5.5.2.2.6 ftp-server timeout 130
5.5.2.2.7 ip ftp 130
5.5.2.2.8 copy（TFTP） 130
5.5.2.2.9 tftp-server enable 131
5.5.2.2.10 tftp-server retransmission-number 132
5.5.2.2.11 tftp-server transmission-timeout 132
5.5.2.3 FTP/TFTP Configuration Examples 132
5.5.2.4 FTP/TFTP Troubleshooting Help 136
5.5.2.4.1 Monitor and Debug Commands 136
5.5.2.4.2 show ftp 136
5.5.2.4.3 show tftp 137
5.5.2.4.4 FTP Troubleshooting Help 137
5.5.2.4.5 TFTP Troubleshooting Help 138
5.6 WEB MANAGEMENT 139
5.6.1 Switch basic configuration 139
5.6.1.1 Basicconfig 139
5.6.1.2 Configure exec timeout 140
5.6.2 SNMP configuration 140
5.6.2.1 SNMP manager configuration 140
5.6.2.2 Trap manager configuration 140
5.6.2.3 Configure IP address of SNMP manager 141

5.6.2.4 SNMP statistics 141
5.6.2.5 RMON and trap configuration 141
5.6.3 Switch upgrade 142
5.6.3.1 TFTP client configuration 142
5.6.3.2 TFTP server configuration 143
5.6.3.3 FTP client configuration 143
5.6.3.4 FTP server configuration 144
5.6.4 Maintenance and debug command 144
5.6.4.1 Debug command 145
5.6.4.2 Show vlan port property 146
5.6.4.3 Others 146
5.6.5 Basic introduction to switch 147
5.6.6 Switch on-off information 147
5.6.7 Switch Maintenance 147
5.6.7.1 Web server user configuration 148
5.6.7.2 Exit current web configuration 148
5.6.7.3 Save current running-config 148
5.6.7.4 Reboot 148
5.6.7.5 Reboot with the default configuration 148
5.6.8 Telnet server configuration 149
5.6.8.1 Telnet server user configuration 149
5.6.8.2 Telnet security IP 149

CHAPTER 6 DEVICE MANAGEMENT 151

6.1 DEVICE MANAGEMENT BRIEF 151
6.2 DEVICE MANAGEMENT CONFIGURATION 151
6.2.1 Switch Basic Configuration 151
6.2.2 Device Management Troubleshooting Help 151
6.2.2.1 Monitor and Debug Commands 151
6.2.2.1.1 show slot 151
6.2.2.1.2 show fan 152
6.2.2.1.3 show power 152
6.2.2.1.4 debug devsm 152
6.3 CARD HOT-SWAP OPERATION 153
6.3.1 Card Hot-Insertion 153
6.3.2 Card Hot-Remove 153
6.3.3 Configuration Recover Rules 153
6.3.4 Active-Standby Alternation 154
6.4 WEB MANAGEMENT 154

6.4.1 Reset specific module *154*
6.4.2 Show slot *154*
6.4.3 Show fan *155*
6.4.4 Show power *155*
6.4.5 Show module in slot *156*

CHAPTER 7 PORT CONFIGURATION 157

7.1 INTRODUCTION TO PORT 157
7.2 PORT CONFIGURATION 158
7.2.1 Network Port Configuration *158*
7.2.1.1 Network Port Configuration Task Sequence 158
7.2.1.2 Ethernet Port Configuration Commands 159
7.2.1.2.1 bandwidth 159
7.2.1.2.2 combo-forced-mode 160
7.2.1.2.3 flow control 161
7.2.1.2.4 interface ethernet 162
7.2.1.2.5 loopback 162
7.2.1.2.6 mdi 162
7.2.1.2.7 name 163
7.2.1.2.8 negotiation 163
7.2.1.2.9 rate-suppression 164
7.2.1.2.10 shutdown 164
7.2.1.2.11 speed-duplex 165
7.2.2 VLAN Interface Configuration *165*
7.2.2.1 VLAN Interface Configuration Task Sequence 165
7.2.2.2 VLAN Interface Configuration Commands 166
7.2.2.2.1 interface vlan 166
7.2.2.2.2 ip address 166
7.2.2.2.3 shutdown 167
7.2.3 Network Management Port Configuration *167*
7.2.3.1 Network Management Port Configuration Task Sequence 167
7.2.3.2 Network Management Port Configuration Commands 168
7.2.3.2.1 duplex 168
7.2.3.2.2 interface ethernet 169
7.2.3.2.3 ip address 169
7.2.3.2.4 loopback 169
7.2.3.2.5 shutdown 170
7.2.3.2.6 speed 170
7.2.4 Port Mirroring Configuration *170*

7.2.4.1 Introduction to Port Mirroring 170
7.2.4.2 Port Mirroring Configuration Task Sequence 171
7.2.4.3 Port Mirroring Configuration 171
7.2.4.3.1 monitor session source interface 171
7.2.4.3.2 monitor session destination interface 172
7.2.4.4 Port Mirroring Examples 172
7.2.4.5 Device Mirroring Troubleshooting Help 172
7.2.4.5.1 Monitor and Debug Commands 173
7.2.4.5.1.1 show monitor 173
7.2.4.5.2 Device Mirroring Troubleshooting Help 173
7.3 PORT CONFIGURATION EXAMPLE 174
7.4 PORT TROUBLESHOOTING HELP 175
7.4.1 Monitor and Debug Commands 175
7.4.1.1 clear counters 175
7.4.1.2 show interface 175
7.4.2 Port Troubleshooting Help 176
7.5 WEB MANAGEMENT 176
7.5.1 Ethernet port configuration 176
7.5.1.1 Physical port configuration 176
7.5.1.2 Bandwidth control 177
7.5.2 Vlan interface configuration 178
7.5.2.1 Allocate IP address for L3 port 178
7.5.2.2 L3 port IP addr mode configuration 178
7.5.3 Port mirroring configuration 179
7.5.3.1 Mirror configuration 179
7.5.4 Port debug and maintenance 179
7.5.4.1 Show port information 180
CHAPTER 8 MAC TABLE CONFIGURATION 181
8.1 INTRODUCTION TO MAC TABLE 181
8.1.1 Obtaining MAC Table 181
8.1.2 Forward or Filter 183
8.2 MAC TABLE CONFIGURATION 184
8.2.1 mac-address-table aging-time 184
8.2.2 mac-address-table static 184
8.2.3 mac-address-table blackhole 185
8.3 TYPICAL CONFIGURATION EXAMPLES 185
8.4 TROUBLESHOOTING HELP 186
8.4.1 Monitor and Debug Commands 186

8.4.1.1 show mac-address-table aging-time 186
8.4.1.2 show mac-address-table static 186
8.4.1.3 show mac-address-table blackhole 187
8.4.2 Troubleshooting Help 187
8.5 MAC ADDRESS FUNCTION EXTENSION 187
8.5.1 MAC Address Binding 187
8.5.1.1 Introduction to MAC Address Binding 187
8.5.1.2 MAC Address Binding Configuration 188
8.5.1.2.1 MAC Address Binding Configuration Task Sequence 188
8.5.1.2.2 MAC Address Binding Configuration Commands 189
8.5.1.2.2.1 switchport port-security 189
8.5.1.2.2.2 switchport port-security convert 189
8.5.1.2.2.3 switchport port-security lock 190
8.5.1.2.2.4 switchport port-security timeout 190
8.5.1.2.2.5 switchport port-security mac-address 191
8.5.1.2.2.6 clear port-security dynamic 191
8.5.1.2.2.7 switchport port-security maximum 191
8.5.1.2.2.8 switchport port-security violation 192
8.5.1.3 Mac Address Binding Troubleshooting Help 192
8.5.1.3.1 MAC Address Binding Debug and Monitor Commands 192
8.5.1.3.1.1 show port-security 192
8.5.1.3.1.2 show port-security interface 193
8.5.1.3.1.3 show port-security address 194
8.5.1.3.2 MAC Address Binding Troubleshooting Help 195
8.6 WEB MANAGEMENT 195
8.6.1 Mac address table configuration 195
8.6.1.1 Unicast address configuration 195
8.6.1.2 Delete unicast address 196
8.6.1.3 MAC address query 196
8.6.1.4 Show MAC address table 197
8.6.2 MAC address binding configuration 198
8.6.2.1 Enable port MAC-Binding 198
8.6.2.1.1 Enable port MAC-Binding 198
8.6.2.2 Lock port 198
8.6.2.2.1 Lock port 198
8.6.2.2.2 Dynamic MAC converting 199
8.6.2.2.3 Enable port security timeout 199
8.6.2.2.4 Binding MAC 199

8.6.2.2.5 Clearing port MAC 200
8.6.2.3 MAC binding attribution configuration 200
8.6.2.3.1 Maximum port security IP number configuration 200
8.6.2.3.2 Port violation mode 200
8.6.2.4 MAC binding debug 201
8.6.2.4.1 Show MAC binding security address 201

CHAPTER 9 VLAN CONFIGURATION 202

9.1 INTRODUCTION TO VLAN 202
9.2 VLAN CONFIGURATION 203
9.2.1 VLAN Configuration Task Sequence 203
9.2.2 VLAN Configuration Commands 204
9.2.2.1 vlan 204
9.2.2.2 name 205
9.2.2.3 switchport access vlan 205
9.2.2.4 switchport interface 205
9.2.2.5 switchport mode 206
9.2.2.6 switchport trunk allowed vlan 206
9.2.2.7 switchport trunk native vlan 207
9.2.2.8 vlan ingress disable 207
9.2.3 Typical VLAN Application 208
9.3 GVRP CONFIGURATION 209
9.3.1 GVRP Configuration Task Sequence 210
9.3.2 GVRP Commands 211
9.3.2.1 garp timer join 211
9.3.2.2 garp timer leave 211
9.3.2.3 garp timer hold 211
9.3.2.4 garp timer leaveall 212
9.3.2.5 gvrp 212
9.3.3 Typical GVRP Application 213
9.4 VLAN TROUBLESHOOTING HELP 215
9.4.1 Monitor and Debug Information 215
9.4.1.1 show vlan 215
9.4.1.2 show garp 216
9.4.1.3 show gvrp 216
9.4.1.4 debug gvrp 216
9.4.2 VLAN Troubleshooting Help 217
9.5 WEB MANAGEMENT 217
9.5.1 Vlan configuration 217

9.5.1.1 Create/remove Vlan 217
9.5.1.1.1 VID allocation 217
9.5.1.1.2 VID attribution configuration 218
9.5.1.2 Allocate port for Vlan 218
9.5.1.2.1 Allocate port for Vlan 218
9.5.1.3 Port type configuration 219
9.5.1.3.1 Set port mode(trunk/access) 219
9.5.1.4 Trunk port configuration 220
9.5.1.4.1 Vlan setting for trunk port 220
9.5.1.5 Set allow Vlan 220
9.5.1.5.1 Vlan setting for access port 220
9.5.1.6 Enable/Disable Vlan ingress rule 221
9.5.1.6.1 Disable Vlan ingress rule 221
9.5.2 GVRP configuration 222
9.5.2.1 Enable global GVRP 222
9.5.2.2 Enable port GVRP 222
9.5.2.3 GVRP configuration 222
9.5.3 Vlan debug and maintenance 223
9.5.3.1 Show vlan 223
9.5.3.2 Show GARP 223
9.5.3.3 Show GVRP 223

CHAPTER 10 MSTP CONFIGURATION 225

10.1 INTRODUCTION TO MSTP 225
10.1.1 MSTP field 225
10.1.1.1 MST field operation 226
10.1.1.2 MST inter-field operation 226
10.1.2 Port role 226
10.2 MSTP CONFIGURATION 227
10.2.1 MSTP configuration task sequence 227
10.2.2 Introduction to MSTP configuration commands 229
10.2.2.1 abort 229
10.2.2.2 exit 229
10.2.2.3 instance vlan 229
10.2.2.4 name 230
10.2.2.5 revision-level 230
10.2.2.6 spanning-tree 231
10.2.2.7 spanning-tree forward-time 231
10.2.2.8 spanning-tree hello-time 231

10.2.2.9 spanning-tree link-type p2p 232
10.2.2.10 spanning-tree maxage 232
10.2.2.11 spanning-tree max-hop 233
10.2.2.12 spanning-tree mcheck 233
10.2.2.13 spanning-tree mode 234
10.2.2.14 spanning-tree mst configuration 234
10.2.2.15 spanning-tree mst cost 235
10.2.2.16 spanning-tree mst port-priority 235
10.2.2.17 spanning-tree mst priority 236
10.2.2.18 spanning-tree portfast 236
10.3 MSTP EXAMPLE 237
10.4 MSTP TROUBLESHOOTING HELP 241
10.4.1 Monitor and Debug Command 241
10.4.1.1 show spanning-tree 241
10.4.1.2 show mst configuration 244
10.4.1.3 show mst-pending 244
10.4.1.4 debug spanning-tree 245
10.4.2 MSTP Troubleshooting Help 245
10.5 WEB MANAGEMENT 246
10.5.1 MSTP field operation 246
10.5.1.1 Instance configuration 246
10.5.1.2 Field operation 246
10.5.1.3 Revision level control 246
10.5.2 MSTP port operation 247
10.5.2.1 Edge port setting 247
10.5.2.2 Port priority setting 247
10.5.2.3 Port route cost setting 247
10.5.2.4 MSTP mode 247
10.5.2.5 Link type configuration 248
10.5.2.6 MSTP port configuration 248
10.5.3 MSTP global control 248
10.5.3.1 MSTP global protocol port configuration 248
10.5.3.2 Forward delay time configuration 248
10.5.3.3 Hello_time configuration 248
10.5.3.4 Set the max age time for BPDU information in the switch 249
10.5.3.5 Set the max hop count support for BPDU transmitting in MSTP field 249
10.5.3.6 Set switch to spanning tree mode 249
10.5.3.7 Set bridge priority of the specified instance for the switch 249

10.5.4 Show MSTP setting *250*
10.5.4.1 Instance information 250
10.5.4.2 MSTP field information 250

CHAPTER11 IGMP SNOOPING CONFIGURATION 251

11.1 INTRODUCTION TO IGMP SNOOPING 251
11.2 IGMP SNOOPING CONFIGURATION 251
11.2.1 IGMP Snooping Configuration Task *251*
11.2.2 IGMP Snooping Configuration Command *252*
11.2.2.1 ip igmp snooping 252
11.2.2.2 ip igmp snooping vlan 253
11.2.2.3 ip igmp snooping vlan mrouter 253
11.2.2.4 ip igmp snooping vlan static 254
11.2.2.5 ip igmp snooping vlan immediate-leave 254
11.2.2.6 ip igmp snooping vlan query 254
11.2.2.7 ip igmp snooping vlan query robustness 255
11.2.2.8 ip igmp snooping vlan query interval 255
11.2.2.9 ip igmp snooping vlan query max-response-time 255
11.3 IGMP SNOOPING EXAMPLE 256
11.4 IGMP SNOOPING TROUBLESHOOTING HELP 258
11.4.1 Monitor and Debug Commands *258*
11.4.1.1 show ip igmp snooping 258
11.4.1.2 show mac-address-table multicast 261
11.4.1.3 debug igmp snooping 261
11.4.2 IGMP Snooping Troubleshooting Help *262*
11.5 WEB MANAGEMENT 262
11.5.1 Turning on the IGMP snooping function *262*
11.5.2 IGMP snooping configuration *263*
11.5.2.1 Query configuration 263
11.5.2.2 Snooping configuration 263
11.5.2.3 Configuration display 263
11.5.3 IGMP snooping static multicast configuration *264*
11.5.3.1 IGMP snooping static multicast configuration 264
11.5.3.2 IGMP snooping display 264

CHAPTER 12 ACL CONFIGURATION 266

12.1 INTRODUCTION TO ACL 266
12.1.1 Access list *266*
12.1.2 Access-group *266*

12.1.3 Access list Action and Global Default Action *266*
12.2 ACL CONFIGURATION 267
12.2.1 ACL Configuration Task Sequence *267*
12.2.2 ACL Configuration Commands *271*
12.2.2.1 access-list(extended) 271
12.2.2.2 access list(standard) 272
12.2.2.3 firewall 272
12.2.2.4 firewall default 272
12.2.2.5 ip access extended 273
12.2.2.6 ip access standard 273
12.2.2.7 ip access-group 273
12.2.2.8 permit | deny(extended) 274
12.2.2.9 permit | deny(standard) 275
12.3 ACL EXAMPLE 275
12.4 ACL TROUBLESHOOTING HELP 276
12.4.1 ACL Debug and Monitor Commands *276*
12.4.1.1 show access lists 276
12.4.1.2 show access-group 277
12.4.1.3 show firewall 277
12.4.2 ACL Troubleshooting Help *278*
12.5 WEB MANAGEMENT 278
12.5.1 Numeric standard ACL configuration *279*
12.5.2 Delete numeric IP ACL *279*
12.5.3 Configure the numeric extended ACL *279*
12.5.4 Configure standard ACL name configuration and delete the standard ACL name configuration *281*
12.5.5 Configure extended ACL name configuration *282*
12.5.6 Firewall configuration *282*
12.5.7 ACL port binding *283*

CHAPTER 13 PORT CHANNEL CONFIGURATION 284

13.1 INTRODUCTION TO PORT CHANNEL 284
13.2 PORT CHANNEL CONFIGURATION 285
13.2.1 Port Channel Configuration Task Sequence *285*
13.2.2 Port Channel Configuration Commands *286*
13.2.2.1 port-group 286
13.2.2.2 port-group mode 287
13.2.2.3 interface port-channel 287
13.3 PORT CHANNEL EXAMPLE 288

13.4 PORT CHANNEL TROUBLESHOOTING HELP 290
13.4.1 Monitor and Debug Commands 290
13.4.1.1 show port-group 290
13.4.1.2 debug lacp 294
13.4.2 Port Channel Troubleshooting Help 295
13.5 WEB MANAGEMENT 295
13.5.1 LACP port group configuration 295
13.5.2 LACP port configuration 296
CHAPTER 14 DHCP CONFIGURATION 297
14.1 INTRODUCTION TO DHCP 297
14.2 DHCP SERVER CONFIGURATION 298
14.2.1 DHCP Sever Configuration Task Sequence 298
14.2.2 DHCP Server Configuration Commands 300
14.2.2.1 bootfile 300
14.2.2.2 client-identifier 300
14.2.2.3 client-name 301
14.2.2.4 default-router 301
14.2.2.5 dns-server 301
14.2.2.6 domain-name 302
14.2.2.7 hardware-address 302
14.2.2.8 host 302
14.2.2.9 ip dhcp conflict logging 303
14.2.2.10 ip dhcp excluded-address 303
14.2.2.11 ip dhcp pool 304
14.2.2.12 loghost dhcp 304
14.2.2.13 lease 304
14.2.2.14 netbios-name-server 305
14.2.2.15 netbios-node-type 305
14.2.2.16 network-address 306
14.2.2.17 next-server 306
14.2.2.18 option 306
14.2.2.19 service dhcp 307
14.3 DHCP RELAY CONFIGURATION 307
14.3.1 DHCP Relay Configuration Task Sequence 308
14.3.2 DHCP Relay Configuration Command 309
14.3.2.1 ip forward-protocol udp 309
14.3.2.2 ip helper-address 309
14.3.2.3 ip dhcp relay information policy drop 309

14.4 DHCP CONFIGURATION EXAMPLE 310
14.5 DHCP TROUBLESHOOTING HELP 313
14.5.1 Monitor and Debug Commands 313
14.5.1.1 clear ip dhcp binding 313
14.5.1.2 clear ip dhcp conflict 313
14.5.1.3 clear ip dhcp server statistics 314
14.5.1.4 show ip dhcp binding 314
14.5.1.5 show ip dhcp conflict 315
14.5.1.6 show ip dhcp server statistics 315
14.5.1.7 debug ip dhcp server 316
14.5.2 DHCP Troubleshooting Help 317
14.6 WEB MANAGEMENT 317
14.6.1 DHCP server configuration 317
14.6.2 Enable DHCP 317
14.6.2.1 Address pool configuration 318
14.6.2.2 Client's default gateway configuration 319
14.6.2.3 Client dns server configuration 319
14.6.2.4 Client wins server configuration 320
14.6.2.5 DHCP file server address configuration 321
14.6.2.6 DHCP network parameter configuration 321
14.6.2.7 Manual address pool configuration 322
14.6.2.8 Excluded address configuration 322
14.6.2.9 DHCP packet statistics 323
14.6.3 DHCP relay configuration 323
14.6.3.1 DHCP relay configuration 324
14.6.4 DHCP debugging 324
14.6.4.1 Delete binding log 324
14.6.4.2 Delete conflict log 325
14.6.4.3 Delete DHCP server statistics log 325
14.6.4.4 Show IP-Mac binding 325
14.6.2.5 Show conflict-logging 325

CHAPTER 15 SNTP CONFIGURATION 326

15.1 SNTP CONFIGURATION COMMANDS 327
15.1.1 sntp server 327
15.1.2 sntp polltime 327
15.1.3 sntp timezone 327
15.2 TYPICAL SNTP CONFIGURATION EXAMPLES 328
15.3 SNTP TROUBLESHOOTING HELP 329

15.3.1 Monitor and Debug Commands *329*
15.3.1.1 show sntp 329
15.3.1.2 debug sntp 329
15.4 WEB MANAGEMENT 329
15.4.1 SNMP/NTP server configuration *329*
15.4.2 Request interval configuration *330*
15.4.3 Time difference *330*
15.4.4 Show SNMP *330*
CHAPTER 16 QOS CONFIGURATION 331
16.1 INTRODUCTION TO QOS 331
16.1.1 QoS Terms *331*
16.1.2 QoS Implementation *332*
16.1.3 Basic QoS Model *332*
16.2 QOS CONFIGURATION 336
16.2.1 QoS Configuration Task Sequence *336*
16.2.2 QoS Configuration Commands *340*
16.2.2.1 mls qos 340
16.2.2.2 class-map 340
16.2.2.3 match 340
16.2.2.4 policy-map 341
16.2.2.5 class 341
16.2.2.6 set 342
16.2.2.7 police 342
16.2.2.8 mls qos aggregate-policer 343
16.2.2.9 police aggregate 343
16.2.2.10 mls qos trust 344
16.2.2.11 mls qos cos 344
16.2.2.12 service-policy 345
16.2.2.13 mls qos dscp-mutation 345
16.2.2.14 wrr-queue bandwidth 346
16.2.2.15 priority-queue out 346
16.2.2.16 wrr-queue cos-map 347
16.2.2.17 mls qos map 347
16.3 QOS EXAMPLE 348
16.4 QOS TROUBLESHOOTING HELP 351
16.4.1 QoS Debug and Monitor Commands *351*
16.4.1.1 show mls-qos 351
16.4.1.2 show mls qos aggregate-policer 351

16.4.1.3 show mls qos interface 352
16.4.1.4 show mls qos maps 353
16.4.1.5 show class-map 355
16.4.1.6 show policy-map 355
16.4.2 QoS Troubleshooting Help 356
16.5 WEB MANAGEMENT 356
16.5.1 Enable QoS 356
16.5.2 Class-map configuration 357
16.5.2.1 Add/Remove class-Map 357
16.5.2.2 Class-map configuration 357
16.5.3 Policy-map priority configuration 358
16.5.3.1 Add/Remove policy-map 358
16.5.3.2 Policy-map priority configuration 359
16.5.3.3 Policy-map bandwidth configuration 359
16.5.3.4 Add/Remove aggregate policy 360
16.5.3.5 Apply aggregate policy 360
16.5.4 Apply QoS to port 361
16.5.4.1 Port trust mode configuration 361
16.5.4.2 Port default CoS configuration 362
16.5.4.3 Apply policy-map to port 362
16.5.4.4 Apply DSCP mutation mapping 362
16.5.5 Egress-queue configuration 363
16.5.5.1 Egress-queue WRR weight configuration 363
16.5.5.2 Egress-queue Work mode configuration 364
16.5.5.3 Mapping CoS values to egress queue 364
16.5.6 QoS mapping configuration 364
16.5.6.1 CoS-to-DSCP mapping 365
16.5.6.2 DSCP-to-CoS mapping 365
16.5.6.3 DSCP mutation mapping 366
16.5.6.4 IP-precedence-to-DSCP mapping 366
16.5.6.5 DSCP mark down mapping 366
CHAPTER 17 L3 FORWARD CONFIGURATION 368
17.1 LAYER 3 INTERFACE 368
17.1.1 Introduction to Layer 3 Interface 368
17.1.2 Layer 3 interface configuration 368
17.1.2.1 Layer 3 Interface Configuration Task Sequence 368
17.1.2.2 Layer 3 Interface Configuration Commands 369
17.1.2.2.1 interface vlan 369

17.2 IP FORWARDING 369
17.2.1 Introduction to IP Forwarding 369
17.2.2 IP Route Aggregation Configuration 369
17.2.2.1 IP Route Aggregation Configuration Task 369
17.2.2.2 IP Route Aggregation Configuration Command 370
17.2.2.2.1 ip fib optimize 370
17.2.3 IP Forwarding Troubleshooting Help 370
17.2.3.1 Monitor and Debug Commands 370
17.2.3.1.1 show ip traffic 370
17.2.3.1.2 debug ip packet 372
17.3 ARP 373
17.3.1 Introduction to ARP 373
17.3.2 ARP configuration 373
17.3.2.1 ARP Configuration Task Sequence 373
17.3.2.2 ARP Forwarding Configuration Commands 373
17.3.2.2.1 Arp 373
17.3.2.2.2 ip proxy-arp 374
17.3.3 ARP Forwarding Troubleshooting Help 374
17.3.3.1 Monitor and Debug Commands 374
17.3.3.1.1 show arp 374
17.3.3.1.2 clear arp-cache 375
17.3.3.1.3 debug arp 375
17.3.3.2 ARP Troubleshooting Help 376
17.4 WEB MANAGEMENT 376
17.4.1 L3 port configuration 376
17.4.2 IP route aggregation configuration 376
17.4.3 ARP configuration 377
17.4.3.1 Configure static ARP 377
17.4.3.2 Clear ARP 377
17.4.3.3 Show ARP 377
17.4.3.4 Proxy ARP configuration 377

CHAPTER 18 ROUTING PROTOCOL CONFIGURATION 378

18.1 ROUTE TABLE 378
18.2 STATIC ROUTE 379
18.2.1 Introduction to Static Route 379
18.2.2 Introduction to Default Route 380
18.2.3 Static Route Configuration 380
18.2.3.1 Static Route Configuration Task Sequence 380

18.2.3.2 Static Route Configuration Commands 380
18.2.3.2.1 ip route 380
18.2.3.2.2 show ip route 381
18.2.4 Configuration Scenario 382
18.2.5 Troubleshooting Help 383
18.2.5.1 Monitor and Debug Commands 383
18.3 RIP 384
18.3.1 Introduction to RIP 384
18.3.2 RIP Configuration 386
18.3.2.1 RIP Configuration Task Sequence 386
18.3.2.2 RIP Configuration Commands 389
18.3.2.2.1 auto-summary 390
18.3.2.2.2 default-metric 390
18.3.2.2.3 ip rip authentication key-chain 391
18.3.2.2.4 ip rip authentication mode 391
18.3.2.2.5 ip rip metricin 391
18.3.2.2.6 ip rip metricout 392
18.3.2.2.7 ip rip input 392
18.3.2.2.8 ip rip output 392
18.3.2.2.9 ip rip receive version 393
18.3.2.2.10 ip rip send version 393
18.3.2.2.11 ip rip work 393
18.3.2.2.12 ip split-horizon 393
18.3.2.2.13 redistribute 394
18.3.2.2.14 rip broadcast 394
18.3.2.2.15 rip checkzero 394
18.3.2.2.16 rip preference 395
18.3.2.2.17 router rip 395
18.3.2.2.18 timer basic 395
18.3.2.2.19 version 396
18.3.2.2.20 show ip protocols 396
18.3.2.2.21 show ip rip 397
18.3.2.2.22 debug ip rip packet 398
18.3.2.2.23 debug ip rip recv 399
18.3.2.2.24 debug ip rip send 399
18.3.3 Typical RIP Scenario 400
18.3.4 RIP Troubleshooting Help 402
18.3.4.1 Monitor and Debug Commands 402

18.3.4.2 RIP Troubleshooting 404
18.4 OSPF 404
18.4.1 Introduction to OSPF 404
18.4.2 OSPF Configuration 407
18.4.2.1 Configuration Task Sequence 407
18.4.2.2 OSPF Configuration Commands 410
18.4.2.2.1 default redistribute cost 411
18.4.2.2.2 default redistribute interval 411
18.4.2.2.3 default redistribute limit 412
18.4.2.2.4 default redistribute tag 412
18.4.2.2.5 default redistribute type 413
18.4.2.2.6 ip ospf authentication 413
18.4.2.2.7 ip ospf cost 413
18.4.2.2.8 ip ospf dead-interval 414
18.4.2.2.9 ospf enable area 414
18.4.2.2.10 ip ospf hello-interval 414
18.4.2.2.11 ip ospf passive-interface 415
18.4.2.2.12 ip ospf priority 415
18.4.2.2.13 ip ospf retransmit-interval 416
18.4.2.2.14 ip ospf transmit-delay 416
18.4.2.2.15 network 416
18.4.2.2.16 preference 417
18.4.2.2.17 redistribute ospfase 417
18.4.2.2.18 router id 418
18.4.2.2.19 router ospf 418
18.4.2.2.20 stub cost 418
18.4.2.2.21 virtuallink neighborid 419
18.4.2.2.22 show ip ospf 419
18.4.2.2.23 show ip ospf ase 420
18.4.2.2.24 show ip ospf cumulative 421
18.4.2.2.25 show ip ospf database 422
18.4.2.2.26 show ip ospf interface 424
18.4.2.2.27 show ip ospf neighbor 425
18.4.2.2.28 show ip ospf routing 426
18.4.2.2.29 show ip ospf virtual-links 426
18.4.2.2.30 show ip protocols 427
18.4.2.2.31 debug ip ospf event 427
18.4.2.2.32 debug ip ospf lsa 428

18.4.2.2.33 debug ip ospf packet 428
18.4.2.2.34 debug ip ospf spf 429
18.4.3 Typical OSPF Scenario 429
18.4.4 OSPF Troubleshooting Help 436
18.4.4.1 Monitor and Debugging Commands 436
18.4.4.2 OSPF Troubleshooting Help 444
18.5 WEB MANAGEMENT 445
18.5.1 Static route 445
18.5.1.1 Static route configuration 445
18.5.2 RIP configuration 445
18.5.2.1 RIP configuration 446
18.5.2.1.1 Enable RIP 446
18.5.2.1.2 Enable port to receive/transmit RIP packet 446
18.5.2.2 RIP parameter configuration 446
18.5.2.2.1 Enable imported route 446
18.5.2.2.2 Metricin/out configuration 447
18.5.2.2.3 RIP imported route 447
18.5.2.2.4 Global RIP configuration 448
18.5.2.2.5 Set RIP timer 449
18.5.3 OSPF 449
18.5.3.1 Enable OSPF protocol 449
18.5.3.1.1 Enable/Disable OSPF protocol 449
18.5.3.1.2 Router-ID configuration 450
18.5.3.1.3 OSPF network range configuration 450
18.5.3.1.4 Configure OSPF area for port 451
18.5.3.2 OSPF TX-parameter configuration 451
18.5.3.2.1 Configure OSPF authentication parameter configuration 451
18.5.3.2.2 Passive interface configuration 452
18.5.3.2.3 Sending packet cost configuration 452
18.5.3.3 OSPF imported route parameter configuration 452
18.5.3.3.1 Imported route parameter configuration 453
18.5.3.3.2 Import external routing information 453
18.5.3.4 Other parameter configuration 453
18.5.3.4.1 OSPF priority configuration 454
18.5.3.4.2 OSPF STUB area and default route cost configuration 454
18.5.3.4.3 OSPF virtual link configuration 454
18.5.3.4.4 Port DR priority configuration 455
18.5.3.5 OSPF debug 455

18.5.4 Display routing table *456*

CHAPTER 19 MULTICAST PROTOCOL CONFIGURATION **457**

19.1 MULTICAST PROTOCOL OVERVIEW 457

19.1.1 Introduction to Multicast *457*

19.1.2 Multicast Address *457*

19.1.3 IP Multicast Packets Forwarding *459*

19.1.4 Application of Multicast *459*

19.2 COMMON MULTICAST CONFIGURATIONS 459

19.2.1 Common Multicast Configuration Commands *459*

19.2.1.1 show ip mroute 460

19.3 PIM-DM 461

19.3.1 Introduction to PIM-DM *461*

19.3.2 PIM-DM Configuration *462*

19.3.2.1 PIM-DM Configuration Task Sequence 462

19.3.2.2 PIM-DM Configuration Commands 462

19.3.2.3 ip pim dense-mode 463

19.3.2.4 ip pim query-interval 463

19.3.3 Typical PIM-DM Scenario *463*

19.3.4 PIM-DM Troubleshooting Help *464*

19.3.4.1 Monitor and Debug Commands 464

19.3.4.2 show ip pim mroute dm 465

19.3.4.3 show ip pim neighbor 466

19.3.4.4 show ip pim interface 466

19.3.4.5 debug ip pim 467

19.3.4.6 PIM-DM Troubleshooting Help 467

19.4 PIM-SM 468

19.4.1 Introduction to PIM-SM *468*

19.4.2 PIM-SM Configuration *469*

19.4.2.1 PIM-SM Configuration Task Sequence 469

19.4.2.2 PIM-SM Configuration Commands 470

19.4.2.2.1 ip pim sparse-mode 471

19.4.2.2.2 ip pim bsr-border 471

19.4.2.2.3 ip pim query-interval 471

19.4.2.2.4 ip pim bsr-candidate 472

19.4.2.2.5 ip pim rp-candidate 472

19.4.3 Typical PIM-SM Scenario *473*

19.4.4 PIM-SM Troubleshooting Help *474*

19.4.4.1 Monitor and Debug Commands 474

19.4.4.1.1 show ip pim bsr-router 474
19.4.4.1.2 show ip pim interface 475
19.4.4.1.3 show ip pim mroute sm 476
19.4.4.1.4 show ip pim neighbor 476
19.4.4.1.5 show ip pim rp 477
19.4.4.1.6 debug ip pim 477
19.4.4.1.7 debug ip pim bsr 478
19.4.4.2 PIM-SM Troubleshooting 479
19.5 DVMRP 479
19.5.1 Introduction to DVMRP 479
19.5.2 DVMRP configuration 480
19.5.2.1 Configuration Task Sequence 480
19.5.2.2 DVMRP Configuration Commands 482
19.5.2.2.1 ip dvmrp cisco-compatible 483
19.5.2.2.2 ip dvmrp enable 483
19.5.2.2.3 ip dvmrp graft-interval 484
19.5.2.2.4 ip dvmrp metric 484
19.5.2.2.5 ip dvmrp nbr-timeout 484
19.5.2.2.6 ip dvmrp probe-interval 485
19.5.2.2.7 ip dvmrp report-interval 485
19.5.2.2.8 ip dvmrp route-timeout 486
19.5.2.2.9 ip dvmrp tunnel 486
19.5.3 Typical DVMRP Scenario 486
19.5.4 DVMRP Troubleshooting Help 487
19.5.4.1 Monitor and Debug Commands 487
19.5.4.1.1 show ip dvmrp mroute 487
19.5.4.1.2 show ip dvmrp neighbor 488
19.5.4.1.3 show ip dvmrp route 489
19.5.4.1.4 show ip dvmrp tunnel 489
19.5.4.1.5 debug ip dvmrp detail 490
19.5.4.1.6 debug ip dvmrp pruning 490
19.5.4.2 DVMRP Troubleshooting 491
19.6 IGMP 492
19.6.1 Introduction to IGMP 492
19.6.2 IGMP configuration 493
19.6.2.1 Configuration Task Sequence 493
19.6.2.2 IGMP Configuration Commands 494
19.6.2.2.1 ip igmp access-group 495

19.6.2.2.2 ip igmp join-group 495
19.6.2.2.3 ip igmp query-interval 496
19.6.2.2.4 ip igmp query-max-response-time 496
19.6.2.2.5 ip igmp query-timeout 496
19.6.2.2.6 ip igmp static-group 497
19.6.2.2.7 ip igmp version 497
19.6.3 Typical IGMP Scenario 498
19.6.4 IGMP Troubleshooting Help 498
19.6.4.1 Monitor and Debug Commands 498
19.6.4.1.1 show ip igmp groups 498
19.6.4.1.2 show ip igmp interface 499
19.6.4.1.3 debug ip igmp event 500
19.6.4.1.4 debug ip igmp packet 500
19.6.4.2 IGMP Troubleshooting 500
19.7 WEB MANAGEMENT 501
19.7.1 Multicast public monitor command 501
19.7.2 PIM-DM configuration 501
19.7.2.1 Enable PIM-DM 501
19.7.2.2 PIM-DM parameter configuration 501
19.7.3 PIM-SM configuration 502
19.7.3.1 Enable PIM-SM 502
19.7.3.2 PIM-SM parameter configuration 502
19.7.3.3 Set interface as PIM-SM BSR border 502
19.7.3.4 Set router as BSR candidate 502
19.7.3.5 Set router as RP candidate 503
19.7.4 DVMRP configuration 503
19.7.4.1 Enable DVMRP 503
19.7.4.2 Cisco-compatible configuration 503
19.7.4.3 DVMRP parameter configuration 504
19.7.4.4 DVMRP global parameter configuration 504
19.7.4.5 DVMRP tunnel configuration 505
19.7.5 IGMP configuration 505
19.7.5.1 IGMP additive parameter configuration 505
19.7.5.2 IGMP version configuration 506
19.7.6 Multicast monitor configuration 506
19.7.6.1 Show ip pim interface 506
19.7.6.2 Show ip pim mroute dm 506
19.7.6.3 Show ip pim neighbor 506

19.7.6.4 Show ip pim bsr-router 506
19.7.6.5 Show ip pim mroute sm 506
19.7.6.6 Show ip pim rp 506
19.7.6.7 Show ip dvmrp mroute 507
19.7.6.8 Show ip dvmrp neighbor 507
19.7.6.9 Show ip dvmrp route 507
19.7.6.10 Show ip dvmrp tunnel 507

CHAPTER20 802.1X CONFIGURATION 508

20.1 INTRODUCTION TO 802.1X 508
20.2 802.1X CONFIGURATION 509
20.2.1 802.1x Configuration Task Sequence 509
20.2.2 802.1x Configuration Commands 512
20.2.2.1 aaa enable 512
20.2.2.2 aaa-accounting enable 513
20.2.2.3 dot1x accept-mac 513
20.2.2.4 dot1x eapor enable 514
20.2.2.5 dot1x enable 514
20.2.2.6 dot1x privateclient enable 514
20.2.2.7 dot1x macfilter enable 515
20.2.2.8 dot1x max-req 515
20.2.2.9 dot1x max-user 515
20.2.2.10 dot1x port-control 516
20.2.2.11 dot1x port-method 516
20.2.2.12 dot1x re-authenticate 516
20.2.2.13 dot1x re-authentication 517
20.2.2.14 dot1x timeout quiet-period 517
20.2.2.15 dot1x timeout re-authperiod 517
20.2.2.16 dot1x timeout tx-period 518
20.2.2.17 radius-server accounting host 518
20.2.2.18 radius-server authentication host 519
20.2.2.19 radius-server dead-time 519
20.2.2.20 radius-server key 520
20.2.2.21 radius-server retransmit 520
20.2.2.22 radius-server timeout 520
20.3 802.1X APPLICATION EXAMPLE 521
20.4 802.1X TROUBLESHOOTING 522
20.4.1 802.1x Debug and Monitor Commands 522
20.4.1.1 show aaa config 522

20.4.1.2 show aaa authenticated-user 523
20.4.1.3 show aaa authenticating-user 524
20.4.1.4 show radius count 524
20.4.1.5 show dot1x 525
20.4.1.6 debug aaa 526
20.4.1.7 debug dot1x 527
20.4.2 802.1x Troubleshooting 527
20.5 WEB MANAGEMENT 528
20.5.1 RADIUS client configuration 528
20.5.1.1 RADIUS global configuration 528
20.5.1.2 RADIUS authentication configuration 529
20.5.1.3 RADIUS accounting configuration 530
20.5.2 802.1X configuration 530
20.5.2.1 802.1X configuration 530
20.5.2.2 802.1X port authentication configuration 531
20.5.2.3 802.1X port mac configuration 532
20.5.2.4 802.1X port status list 532

CHAPTER21 VRRP CONFIGURATION 534

21.1 INTRODUCTION TO VRRP 534
21.1.1 Configuration Task Sequence 534
21.1.2 VRRP Configuration Commands 536
21.1.2.1 router vrrp 536
21.1.2.2 virtual-ip 537
21.1.2.3 interface 537
21.1.2.4 enable 537
21.1.2.5 disable 538
21.1.2.6 vrrp authentication mode 538
21.1.2.7 vrrp authentication string 538
21.1.2.8 preempt 539
21.1.2.9 priority 539
21.1.2.10 advertisement-interval 539
21.1.2.11 circuit-failover 540
21.2 TYPICAL VRRP SCENARIO 540
21.3 VRRP TROUBLESHOOTING HELP 541
21.3.1 Monitor and Debug Commands 541
21.3.1.1 show vrrp 541
21.3.1.2 debug vrrp 542
21.3.2 VRRP Troubleshooting Help 543

21.4 WEB MANAGEMENT 543
21.4.1 Create VRRP Number *543*
21.4.2 Configure VRRP Dummy IP *543*
21.4.3 Configure VRRP Port *544*
21.4.4 Activate Virtual Router *544*
21.4.5 Configure Preemptive Mode For VRRP *544*
21.4.6 Configure VRRP priority *544*
21.4.7 Configure VRRP Timer interval *545*
21.4.8 Configure VRRP Interface Monitor *545*
21.4.9 Configure Authentication Mode For VRRP *545*
21.4.10 Configure Authentication String For VRRP *546*

Chapter 1 Product Overview

RECOMMENDATION: Please read this manual first before using the switch, following the instructions to avoid damaging the device.

1.1 Product Brief

Fig 1-1 ES4704BD Switch

1.1.1 Introduction

Edge-Core ES4704BD is a high performance routing switch that can be deployed as a core layer device for campus and enterprise networks, or an aggregation device for IP metropolitan area networks (MAN).

ES4704BD provides 4 slots, 3 or 2 of which are interface module slots. ES4704BD supports various types of line cards, and can seamlessly support network interfaces from 100Mb, 1000Mb to 10Gb Ethernet. Featuring functions such as policy-based routing, IPv6, MPLS, load balance, VPN and Firewall, it is capable of flexibly meeting the different requirements of complex customer environments. Furthermore, ES4704BD allows redundancy for management modules, power supply. It supports both AC-input and DC-input* power supplies, with hot-swapping support for cards, power supplies and fans. The working temperature of all cards can be monitored in real-time, offering carrier-class reliability.

1.1.2 Features

- **Advanced Architecture**

The design for the ES4704BD core routing switch is fully distributed architecture. With a powerful ASIC chip dedicated to high-speed route lookup and traffic forwarding through “longest-match” and “packet-by-packet” mode, the switch ensures enhanced forwarding performance and scalability. ES4704BD can effectively block network viruses such as "Code red”, "Worm.Blaster” and "Worm.Sasser” etc, and is a great choice for large scale networks with busy transactions and complex traffic, therefore meeting the metro-trend for Ethernet.

■ Interfaces

ES4704BD provides 4 slots, and can be configured in Primary controller-Primary Backup mode with 2 management modules and 2 network modules, or Single controller mode with 1 management module and 3 network modules.

■ Carrier Class Reliability

To meet the strict requirements for device reliability of carrier class networks and to ensure 100% uptime of network cores, the design of ES4704BD enables redundancy for all critical parts, such as power supply, management modules and network links, all modules are also hot-swappable, and working temperatures of all parts are monitored real-time.

■ Support for 10G Ethernet

10Gb Ethernet (10GbE) is a leap of Ethernet in both speed and distance, in which full-duplex technology is employed, thus avoiding low-speed, half-duplex CSMA/CD protocol. Moreover, 10GbE maintains the essence of the original Ethernet model, therefore can integrate with the current Ethernet environment seamlessly. ES4704BD supports multi-port 10Gb fiber modules, providing wider bandwidth and more powerful processing capacity, therefore simplifying network structure and lowering network infrastructure cost. It is an ideal solution for MAN/WAN applications.

■ MAC Address Control

In addition to the standard MAC address dynamic learning, ES4704BD introduces several MAC table-based management functions. MAC address binding achieves secure access through the curb of connecting MAC address on the ports. The MAC filtering function can screen unauthorized access devices through MAC address filtering.

■ VLAN Configuration

ES4704BD support standard IEEE802.1Q VLAN, port-based VLAN and GVRP VLAN. IEEE802.1Q VLAN can divide ports into up to 4094 VLAN groups. When IEEE802.1Q VLAN tagging is used, cross-switch VLAN grouping can be enabled to manage broadcasting traffic, offer better security and improved network performance. GARP VLAN Registration Protocol (GVRP) based VLANs can achieve dynamic VLAN registration via GARP (Generic Attribute Registration Protocol), therefore a more flexible VLAN application results by reducing VLAN configurations due to less VLAN configuration changes.

■ Layer 3 Forwarding

Layer 3 forwarding is the forwarding of Layer 3 packets (IP packet) across VLANs, which ES4704BD uses switch chip hardware to forward IP packets, facilitating the on-chip host route entries and default routing table entries, allowing IP packets to be forwarded at full wire speed.

■ Layer 3 Routing Protocols

ES4704BD supports static routing (RIP, OSPF and BGP routing protocols) and Multicast Protocols (IGMP, IGMP Snooping, PIM-SM, PIM-DM and DVMRP) and MPLS, MPLS VPN, MPLS TE, Policy Routing, IPv6, Load Balance and Firewall etc.

■ QoS

ES4704BD supports various QoS policies. It provides 8 priority queues for each port with bandwidth that can be individually set. WRR/SP/SWRR scheduling are also supported. Traffic can be sorted by ports, VLAN, DSCP, IP precedence and ACL, etc. By assigning different DSCP, IP priorities and bandwidth, different service quality for voice, data and video transmissions can be achieved.

■ ACL

ES4704BD supports standard and extended ACLs. ACL is an IP packets filtering mechanism employed by switches, providing network traffic control by granting or denying access through the switches, and thus effectively safeguarding the security of networks. ES4704BD can filter inbound IP-based traffic by source/destination IP/Mac addresses, IP protocol types, TCP/IP port numbers, IP Precedence and ToS information.

■ IEEE802.1x Access Authentication

ES4704BD supports port-based IEEE802.1x access authentication. Access authentication can be managed by number of client per port and dynamic secure authentication based on MAC addresses..

■ Spanning Tree

ES4704BD provides support for IEEE 802.1D Spanning Tree Protocol (STP), IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), and IEEE802.1s Multiple Spanning Tree Protocol (MSTP). Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

■ Bandwidth Management (Port bandwidth Limit)

ES4704BD features upstream and downstream bandwidth management for both, enabling different access bandwidth to be specified according to user levels. Each port can be assigned with different bandwidth to meet the management demands of Access networks.

■ Trunk Port

Trunk port of IEEE802.3ad is supported by ES4704BD. A Trunk group of 2 to 8 ports can be established for link redundancy and load balance.

■ IGMP Snooping

ES4704BD supports IGMP Snooping based on multi-casting applications enabling various multi-cast services (e.g. multimedia playback, remote education and recreation) in an access network with lowered network traffic.

■ Broadcast Storm Control

ES4704BD can effectively prevent broadcast storms from wasting bandwidth with packet level Broadcast Storm Control function, resulting in improved overall system performance.

■ Port Mirroring

ES4704BD supports Port Mirroring, which is used to mirror the inbound and/or outbound traffic on specific port(s) to another port to gather related statistics, which is useful in troubleshooting and traffic monitoring.

■ DHCP Server, Relay and Client

ES4704BD supports a DHCP Server. It can dynamically assign IP addresses to hosts or MAC addresses, and specified IP addresses to implement MAC-IP binding.

■ RADIUS

ES4704BD supports RADIUS (Remote Dial-In User Service) authentication, enabling users to be authenticated via IEEE802.1x protocols.

■ Comprehensive Network Management

With ES4704BD, in-band and out-of-band management can be done through Console, Telnet and SNMP. Console and Telnet management provides simple and easy CLI (command line interface).

SNMP management is V1 and V2C compliant, supporting Ether-Like MIB, Bridge MIB and MIB II, and RMON 1/2/3/9 MIB. With Edge-Core's ECview, full SNMP network management is available. Furthermore, ES4704BD provides a unique workstation IP setting management, enabling the switch to filter unauthorized remote network administrative connections, and keep the validity, security and consistency of remote network management.

1.1.3 Main Features

- 4 slots that can be configured in Primary controller-Primary Backup mode with 2 management modules and 2 network modules, or Single controller mode with one management module and 3 network modules.
- Store-and-forward switching, ensuring minimal latency
- Auto MDI/MDI-X, enabled on all RJ-45 ports, allows connections to other switches using a non-crossover twisted pair cable.
- Full-duplex IEEE802.3x flow control, half-duplex backpressure flow control
- Console management port provided
- Port working status and statistics available
- Restart and reset to factory setting can be done both locally and remotely
- TFTP /FTP firmware upgrade available
- Can be installed into standard 19-inch chassis

1.2 Technical specifications

■ Protocols and Standards

☐ IEEE802.3 10BASE-T Ethernet
☐ IEEE802.3u 100BASE-TX/FX Fast Ethernet
☐ IEEE802.3x Flow control
☐ IEEE802.1x access control
☐ IEEE802.1D/w Spanning Tree
☐ IEEE802.1p Class of Service
☐ IEEE802.1Q VLAN
☐ IEEE802.3ad Link Aggregation
☐ TFTP/FTP
☐ DHCP
☐ BootP
☐ Telnet
☐ IP/UDP/TCP/ICMP
☐ HTTP
☐ SNMP V1/V2C
☐ RIP
☐ OSPF

■ Management Protocols and Methods

☐ CLI command line
☐ SNMP V1/V2C enabled, available through Network management systems such as ECview
☐ Telnet management enabled
☐ RFC1757 RMON（1, 2, 3, 9）

■ MIB Library

☐ RFC1213 MIB II
☐ RFC1493 Bridge MIB
☐ RFC1643 Ether-Like MIB
☐ Edge-Core Private MIB

1.3 Physical Specifications

■ Management Port

☐ One RJ-45 serial port for each management module

■ AC Power Input

☐ 200 ~ 264VAC, 50 ~ 60Hz
☐ Built-in Universal Power Supply

■ Power Consumption

☐ 300W Max

■ Operating Temperature

☐ 0°C ~ 40°C

■ Storage Temperature

☐ -40°C ~ 70°C

■ Relative humidity

☐ 10% ~ 90% with no condensate

■ Dimension

☐ 445mm x 266mm x 421mm (W x H x D)

■ Weight

☐ 30kg (max. full configuration weight)

■ Mean Time Before Failure

☐ Min. 80,000 Hours MTBF

1.4 Hardware Components

ES4704BD consists of the chassis, power supply system, ventilation system, system board, etc.

1.4.1 Chassis

The ES4704BD uses a 19-inch Rack Mountable Chassis, with the standard dimensions of 445mm(W) x 266(H) x 421mm(D). The chassis consists of functional block and power supply block. The function module block is a board rack, which is the supporting structure for ES4704BD system boards (4 boards max). The fan block is located on the left side of the board rack, allowing one fan tray (4 axial fans for each fan tray). Dust gauze is provided on the right of the board rack for filtering air circulation through the rack. The power block upper the dust gauze provides power to the system, supporting up to two power modules. The power modules insert into the power slots from the front, with the distribution box at the back of the rack for maintenance. In addition, there is a ESD Wrist Strap Connectors on the board rack, located on the left side of the upper.

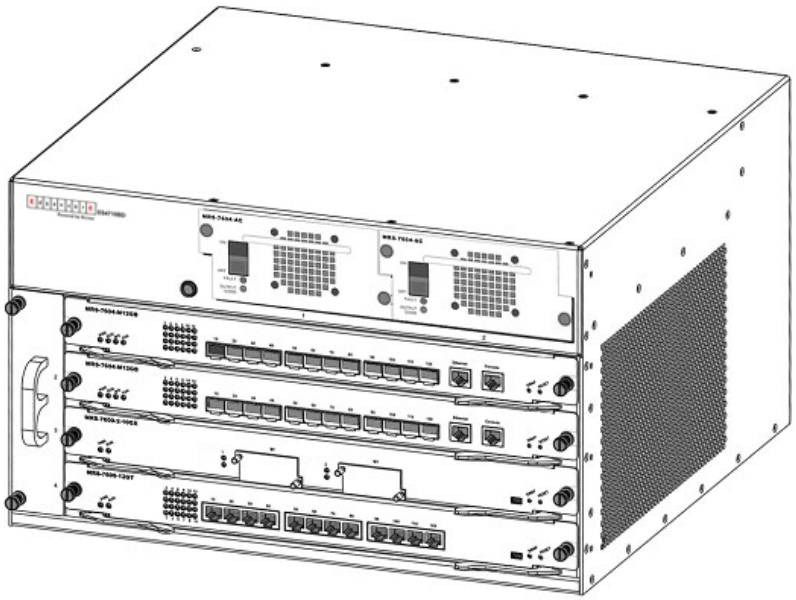


Fig 1-2 ES4704BD Module Outlook

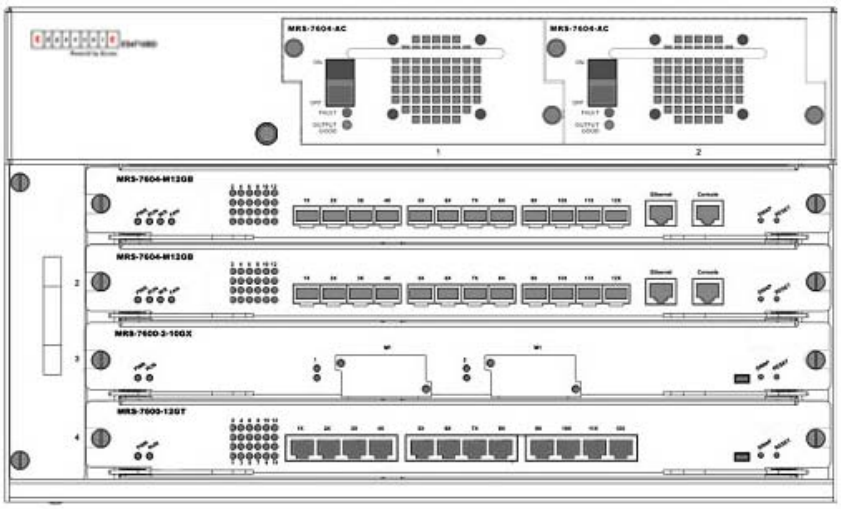


Fig 1-3 ES4704BD Front Panel View

- Management slot: It supports two management slots. EM4704BD-M24TX4GC or EM4704BD-12GX-SFP can be inserted in to the Management slots.The second slot can also be used as I/O slot for configuring various I/O modules, such as EM4700BD-12GT-SFP , EM4700BD-12GT-RJ45 ，EM4700BD-2XG-Xenpak and more.
- Network slot: 2 network slots are provided. Various network modules can be added to the network slots, such as EM4700BD-12GT-RJ45, EM4700BD-12GX-SFP, EM4700BD-2XG-Xenpak,etc.
- Power slot: used for system power supply modules. Supports up to two 300W AC modules.
- Fan tray slot: supports up to one system fan assemblies, each assembly consists of four axial fans.
- Dust gauze slot: exterior air inlet for the ventilation subsystem.
- Distribution box slot: for system distribution box use, works in AC mode based on the power modules.

1.4.1.1 Board Rack

The board rack consists of board slots and a system board.

The boards are inserted vertically into the ES4704BD 4 unit boards are provided. There are four slots in ES4704BD from number 1 to number 4 in order of top to down. The first slot is used to install management module; the second slot is used to management module under 1+1 redundant backup mode or install various I/O interface modules.

A reset button (printed on the panel as ***Reset***), hot swap button (printed on the panel as ***SWAP***), board power indicator (printed on the panel as ***PWR***) and board running status indicator (printed on the panel as ***RUN***) are provided for each board. On the Main Control cards there is Master-Slave indicator (printed on the panel as ***M/S***) There is also a power module status indicator (printed on the panel as ***Power***), fan assembly status indicator (printed on the panel as ***Fan***), and interface status indicators for corresponding management interfaces and network interfaces (printed on the panel as ***Link*** and ***Act***).

The ES4704BD system board is an essential part of the switch, located inside the switch and

providing interconnectivity between the management switch modules (short for *management card*) and network interface modules (*line card*), and for all management and control signals.

1.4.1.2 Power Supply

When using A.C. power supply, we shall adopt power supply of 200~264v and corresponding A.C. distribution box. The permissible range of power supply is ±20%, 50Hz~60Hz. The maximum output power of single power supply module is 300W.

1.4.1.3 Ventilation and Cooling System

The operating ambient temperature of the ES4704BD is 0 ~ 40°C, the thermal design of the equipment can ensure that the surface temperature of the device will not exceed the 50°C to 80°C, the highest temperature allowable.

The switch uses fan assemblies to disperse heat, with the air flow being drawn in through the right section and out through the left section to facilitate air circulation, so that the switch can maintain normal operation under specified environmental conditions. The fan tray is attached to the fan tray slots left the board rack, and ventilation is provided via 4 axial fans that pump out air. Fan trays are hot swappable for maintenance, their status are indicated by the FAN indicators on the main switch panel. In addition, dust gauze is provided on the right of the board rack for filtering the air circulating through the rack. The dust gauze can be unplugged and removed through the back for maintenance.

1.4.2 Introduction to ES4704BD cards

The following six cards for the ES4704BD are currently available:

- Main control card（EM4704BD-M12GX-SFP）： The central switching and controlling module for the ES4704BD, System status control, switch management, user access control and administration, and network operation maintenance are performed here. 12 Gigabit SFP ports are also provided.
- Main control card（EM4704BD-M24TX4GC）： The central switching and controlling module for the ES4704BD, System status control, switch management, user access control and administration, and network operation maintenance are performed here. 24 10/10Base-TX ports with 4 Gigabit combo ports(RJ45or SFP) are also provided.
- 12 copper Gb ports line card (EM4700BD-12GT-RJ45): supporting 12 1000Base-T copper ports for layer 2 and layer 3 switching and routing.
- 12 fiber Gb ports line card (EM4700BD-12GX-SFP): supporting 12 SFP Gb fiber ports for layer 2 and layer 3 switching and routing.
- Dual 10Gb fiber line card (EM4700BD-2XG-XENPAK): supporting 2 10GBase-X fiber ports (XENPAK) for layer 2 and layer 3 switching and routing.

1.4.2.1 EM4704BD-M12GX-SFP

The EM4704BD-M12GX-SFP is switching module for the ES4704BD. System status control, switch management, user access control and administration, and network maintenances are performed here. The board can be inserted into first or second slots of the chassis for Master-Slave redundancy. 12 Gigabit SFP ports are also provided.

1.4.2.1.1 Front Panel

The EM4704BD-M12GX-SFP provides 12 1000Base-SFP ports. At the same time, it comes with 1 Console port (control console) and 1 10/100Base-Tx Ethernet port (administration port).
The Front Panel view is shown below:

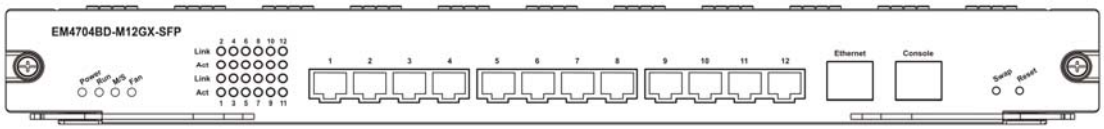


Fig 1-4 EM4704BD-M12GX-SFP Front Panel View

1.4.2.1.2 Front Panel - Indicator

The following table describes the front panel indicators of EM4704BD-M12GX-SFP:

Table 1.1 EM4704BD-M12GX-SFP indicators description

LED	Panel Symbol	Status	Description
Power Indicator	PWR	On (Green)	Card powered
		Off	Card powered off
Operation indicator	RUN	On (Green, blink at 1 Hz)	Cards operating normally
		On (Green, blink at 8 Hz)	System is loading (Booting after cards hot swapping)
		On (Yellow, blink at 8 Hz)	System is shutting down (Shutting Down after *SWAP* button pressed)
		On (Red, blink at 8 Hz)	Cards malfunction
		Off	Cards are powered off and can be removed
Master-Slave indicator	M/S	On (Green)	Master
		Off	Slave
Fan Assembly Status indicator: FAN	OK	On (Green)	Fan operating normally
		Off	Fan malfunctioning or not present (with ***Alarm*** off)
SFP port indicator			
Status indicator	Link	On (Green)	Network connection on SFP transceiver is normal
		Off	No network connection present on SFP transceiver

Transmission Indicator	Act	Blinking (Green)	Sending or receiving data

1.4.2.1.3 Front Panel Port Description

The EM4704BD-M12GX-SFP provides 12 SFP (Mini GBIC) Gigabyte fiber transceiver slots.

The following SFP transceivers are supported by the EM4704BD-M12GX-SFP:

- SFP-SX transceiver
- SFP-LX 10km transceiver
- SFP-LH-40 40km mid-range transceiver
- SFP-LH-70 70km long-range transceiver
- SFP-LH-120 120 km ultra long-range transceiver

The transmission distance for the above transceivers are listed in table 1.2.

Table 1.2 EM4704BD-M12GX-SFP port description

Port Type	Specification
SFP	● SFP-SX transceiver: 62.5/125 μm multi-mode fiber: 275 m 50.0/125 μm multi-mode fiber: 550m ● SFP-LX transceiver: 9/125 μm single-mode fiber: 10 km ● SFP-LH-40 transceiver: 9/125 μm single-mode fiber: 40 km ● SFP-LH-70 transceiver: 9/125 μm single-mode fiber: 70 km ● SFP-LH-120 transceiver: 9/125 μm single-mode fiber: 120 km

1.4.2.1.4 Front Panel – Console Port

The EM4704BD-M12GX-SFP provides a RJ-45 (receptacle) Console serial port. Users can connect to hosts via this port to perform system debugging, configuration, maintenance, administration and host software loading.

Table 1.3 EM4704BD-M12GX-SFP Console description

Property	Specification
Connector	RJ-45 (receptacle)
Connector type	RS-232
Baud rate	9600bps (default)

Supporting service	● Connects to character terminals ● Connects to PC serial port and running terminal emulator on PC.

1.4.2.1.5 Front Panel – Management Port

The EM4704BD-M12GX-SFP provides a RJ-45 (receptacle) Ethernet port. Users can connect through this administration port to hosts for program loading or to connect to remote devices for remote administration (e.g., an administrative workstation). Note: when connecting to the host, a cross-over cable should be used.

Table 1.4 EM4704BD-M12GX-SFP administrative port description

Property	Specification
Connector	RJ-45 (Receptacle)
Connector type	● 10/100Mbps auto sensing ● Cat 5 UTP: 300 m

1.4.2.1.6 Front Panel – Reset Button

EM4704BD-M12GX-SFP provides a RESET button for resetting the board.

1.4.2.1.7 Front Panel – SWAP Button

The EM4704BD-M12GX-SFP provides a SWAP button for hot swapping the module during operation. Before removing the modules, users should press ***SWAP*** button first. The module will then prepare for hot-swap and the system operation indicator (RUN) will turn yellow and blink at 8 Hz. When the ***RUN*** indicator is off, the cards are powered off and can be removed.

1.4.2.2 EM4704BD-M24TX4GC

The EM4704BD-M24TX4GC is switching module for the ES4704BD. System status control, switch management, user access control and administration, and network maintenances are performed here. The board can be inserted into first or second slots of the chassis for Master-Slave redundancy. 24 10/10Base-TX ports with 4 Gigabit combo ports(RJ45or SFP) are also provided.

1.4.2.2.1 Front Panel

The EM4704BD-M24TX4GC provides 24 10/100Base-TX ports and 4 Gigabit COMBO slots. At the same time, it comes with 1 Console port (control console) and 1 10/100Base-Tx Ethernet port (administration port).

The Front Panel view is shown below:

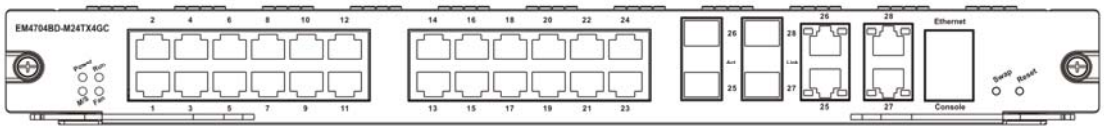


Fig 1-5 EM4704BD-M24TX4GC

1.4.2.2.2 Front Panel - Indicator

The following table describes the front panel indicators of EM4704BD-M24TX4GC:

Table 1.5 EM4704BD-M24TX4GC indicators description

LED	Panel Symbol	Status	Description
Power Indicator	PWR	On (Green)	Card powered
		Off	Card powered off
Operation indicator	RUN	On (Green, blink at 1 Hz)	Cards operating normally
		On (Green, blink at 8 Hz)	System is loading (Booting after cards hot swapping)
		On (Yellow, blink at 8 Hz)	System is shutting down (Shutting Down after *SWAP* button pressed)
		On (Red, blink at 8 Hz)	Cards malfunction
		Off	Cards are powered off and can be removed
Master-Slave indicator	M/S	On (Green)	Master
		Off	Slave
Fan Assembly Status indicator: FAN	FAN	On (Green)	Fan operating normally
		On (Red)	Fan malfunctioning
		Off	Fan not present (with ***Alarm*** off)
SFP port indicator			
Status indicator	Link	On (Green)	Network connection on SFP transceiver is normal
		Off	No network connection present on SFP transceiver
Transmission Indicator	Act	Blinking (Green)	Sending or receiving data
10/100Base-RJ45 port indicator			
Status indicator	Link	On (Green)	Network connection is normal

		Off	No network connection present on 10/100Base-RJ45 port
Transmission Indicator	Act	Blinking (Green)	Sending or receiving data
1000Base-TX port indicator			
Status indicator	Link	On (Green)	Network connection on 1000Base-TX transceiver is normal
		Off	No network connection present on 1000Base-TX transceiver
Transmission Indicator	Act	Blinking (Green)	Sending or receiving data

1.4.2.2.3 Front Panel Port Description

The EM4704BD-M24TX4GC provides 24 10/100Base-TX ports and 4 Gigabite COMBO (RJ-45 or SFP) transceiver slots.

The following SFP transceivers are supported by the EM4704BD-M24TX4GC:

- SFP-SX transceiver
- SFP-LX 10km transceiver
- SFP-LH-40 40km mid-range transceiver
- SFP-LH-70 70km long-range transceiver
- SFP-LH-120 120 km ultra long-range transceiver

The transmission distance for the above transceivers are listed in table 1.2.

Table 1.6 EM4704BD-M24TX4GC port description

Port Type	Specification
SFP	● SFP-SX transceiver: 62.5/125 μm multi-mode fiber: 275 m 50.0/125 μm multi-mode fiber: 550m ● SFP-LX transceiver: 9/125 μm single-mode fiber: 10 km ● SFP-LH-40 transceiver: 9/125 μm single-mode fiber: 40 km ● SFP-LH-70 transceiver: 9/125 μm single-mode fiber: 70 km ● SFP-LH-120 transceiver: 9/125 μm single-mode fiber: 120 km

1.4.2.2.4 Front Panel – Console Port

The EM4704BD-M24TX4GC provides a RJ-45 (receptacle) Console serial port. Users can connect to hosts via this port to perform system debugging, configuration, maintenance, administration and host software loading.

Table 1.7 EM4704BD-M24TX4GC Console description

Property	Specification
Connector	RJ-45 (receptacle)
Connector type	RS-232
Baud rate	9600bps (default)
Supporting service	● Connects to character terminals ● Connects to PC serial port and running terminal emulator on PC.

1.4.2.2.5 Front Panel – Management Port

The EM4704BD-M24TX4GC provides a RJ-45 (receptacle) Ethernet port. Users can connect through this administration port to hosts for program loading or to connect to remote devices for remote administration (e.g., an administrative workstation). Note: when connecting to the host, a cross-over cable should be used.

Table 1.8 EM4704BD-M24TX4GC administrative port description

Property	Specification
Connector	RJ-45 (Receptacle)
Connector type	● 10/100Mbps auto sensing ● Cat 5 UTP: 300 m

1.4.2.2.6 Front Panel – Reset Button

EM4704BD-M24TX4GC provides a RESET button for resetting the board.

1.4.2.2.7 Front Panel – SWAP Button

The EM4704BD-M24TX4GC provides a SWAP button for hot swapping the module during operation. Before removing the modules, users should press ***SWAP*** button first. The module will then prepare for hot-swap and the system operation indicator (RUN) will turn yellow and blink at 8 Hz. When the ***RUN*** indicator is off, the cards are powered off and can be removed.

1.4.2.3 EM4700BD-12GT-RJ45

12 copper Gb ports line card (EM4700BD-12GT-RJ45): supports 12 1000Base-T copper ports for layer 2 and layer 3 switching and routing.

1.4.2.3.1 Front Panel

The EM4700BD-12GT-RJ45 provides 12 RJ45 ports (10/100/1000Mbps adaptive).

The Front Panel view is shown below:

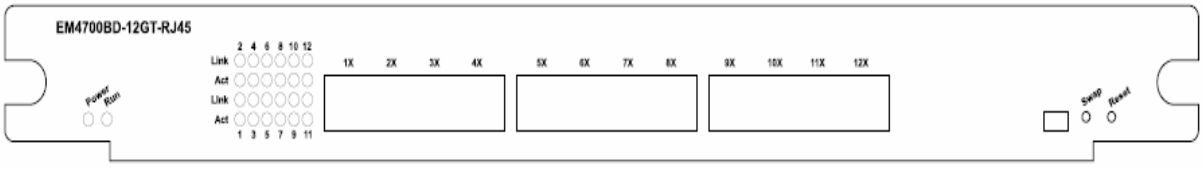


Fig 1-6 EM4700BD-12GT-RJ45 Front Panel view

1.4.2.3.2 Front Panel - Indicator

The following table describes the EM4700BD-12GT-RJ45's front panel indicators:

Table 1.9 EM4700BD-12GT-RJ45 indicator descriptions

LED	Panel Symbol	Status	Description
Power Indicator	PWR	On (green)	Card powered
		Off	Card powered off
Operation indicator	RUN	On (Green, blinks at 1 Hz)	Card operating normally
		On (Green, blinks at 8 Hz)	System is loading (Booting after card hot swapping)
		On (Yellow, blinks at 8 Hz)	System is shutting down (Shutting Down after *SWAP* button pressed)
		On (Red, blinks at 8 Hz)	Malfunction status
		Off	Card is powered off and can be removed
RJ-45 port indicator			
Status indicator	Link	On (Green)	Network connection is normal
		Off	No network connection present on 1000Base-TX port
Transmission Indicator	Act	Blinking (Green)	Sending or receiving data

1.4.2.3.3 Front Panel Port Description

The EM4700BD-12GT-RJ45 provides 12 RJ45 copper Gb ports.

Table 1.10 EM4700BD-12GT-RJ45 port description

Port Type	Specification
RJ-45 port	● 10/100/1000 Mbps auto sensing ● MDI/MDI-X cable ant sensing ● Cat 5 UTP: 100 m

1.4.2.3.4 Front Panel – Reset Button

The EM4700BD-12GT-RJ45 provides a ***RESET*** button for resetting the board.

1.4.2.3.5 Front Panel – SWAP Button

The EM4700BD-12GT-RJ45 provides a SWAP button for hot swapping the module during operation. Before removing the module, users should press the SWAP button first. The module will then prepare for a hot-swap and the system operation indicator (RUN) will turn yellow and blink at 8 Hz. When the ***RUN*** indicator is off, the card is powered off and can be removed.

1.4.2.4 EM4700BD-12GX-SFP

12 fiber Gb ports line card (EM4700BD-12GX-SFP): supports 12 SFP Gb fiber ports for layer 2 and layer 3 switching and routing.

1.4.2.4.1 Front Panel

EM4700BD-12GX-SFP provides 12 SFP ports.

The Front Panel view is shown below:

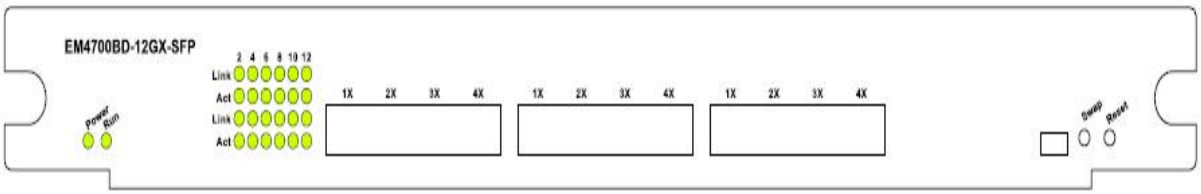


Fig 1-7 EM4700BD-12GX-SFP Front Panel view

1.4.2.4.2 Front Panel - Indicator

The following table describes the EM4700BD-12GX-SFP's front panel indicators:

Table 1.11 EM4700BD-12GX-SFP indicator descriptions

LED	Panel Symbol	Status	Description
Power Indicator	PWR	On (green)	Card powered
		Off	Card powered off
Operation	RUN	On (Green, blinks at 1 Hz)	Cards operating normally

indicator		On (Green, blinks at 8 Hz)	System is loading (Booting after cards hot swapping)
		On (Yellow, blinks at 8 Hz)	System is shutting down (Shutting Down after *SWAP* button pressed)
		On (Red, blinks at 8 Hz)	Malfunction status
		Off	Cards is powered off and can be removed
SFP port indicator			
Status indicator	Link	On (Green)	Network connection on SFP transceiver is normal
		Off	No network connection present on SFP transceiver
Transmission Indicator	Act	Blinking (Green)	Sending or receiving data

1.4.2.4.3 Front Panel Port Description

The EM4700BD-12GX-SFP provides 12 SFP (Mini GBIC) Gigabyte fiber transceiver slots.

The following SFP transceivers are supported by the EM4700BD-12GX-SFP:

- SFP-SX transceiver
- SFP-LX 10km transceiver
- SFP-LH-40 40km mid-range transceiver
- SFP-LH-70 70km long-range transceiver
- SFP-LH-120 120 km ultra long-range transceiver

The transmission distance for the above transceivers are listed in table 1.2.

Table 1.12 EM4700BD-12GX-SFP port description

Port Type	Specification
SFP	● SFP-SX transceiver: 62.5/125 μm multi-mode fiber: 275 m 50.0/125 μm multi-mode fiber: 550m ● SFP-LX transceiver: 9/125 μm single-mode fiber: 10 km ● SFP-LH-40 transceiver: 9/125 μm single-mode fiber: 40 km ● SFP-LH-70 transceiver: 9/125 μm single-mode fiber: 70 km ● SFP-LH-120 transceiver: 9/125 μm single-mode fiber: 120 km

1.4.2.4.4 Front Panel – Reset Button

The EM4700BD-12GX-SFP provides a ***RESET*** button for resetting the board.

1.4.2.4.5 Front Panel – SWAP Button

The EM4700BD-12GX-SFP provides a SWAP button for hot swapping the module during operation. Before removing the modules, users should first press the ***SWAP*** button. The module will then prepare for a hot-swap and the system operation indicator (RUN) will turn yellow and blink at 8 Hz. When the ***RUN*** indicator is off, the cards are powered off and can be removed.

1.4.2.5 EM4700BD-2XG-XENPAK

Dual 10GbE fiber line card (EM4700BD-2XG-XENPAK): supporting 2 XENPAK 10Gb fiber port for layer 2 and layer 3 switching and routing.

1.4.2.5.1 Front Panel

The EM4700BD-2XG-XENPAK provides 2 XENPAK 10Gb fiber transceiver ports, the front panel view is shown below:

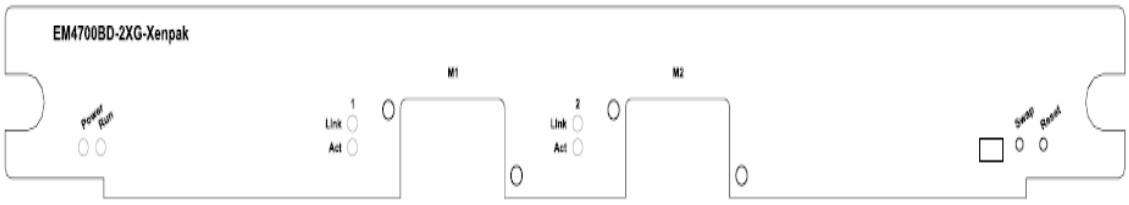


Fig 1-8 EM4700BD-2XG-XENPAK front panel view

1.4.2.5.2 Front Panel - Indicator

The following table describes the front panel indicators for the EM4700BD-2XG-XENPAK:

Table 1.13 Description of the EM4700BD-2XG-XENPAK indicators

LED Indicator	Panel Symbol	Status	Description
Power Indicator	PWR	On (green)	Card powered.
		Off	Card powered off
Operation indicator	RUN	On (Green, blinks at 1 Hz)	Card operating normally
		On (Green, blinks at 8 Hz)	System is loading (Booting after cards hot swapping)
		On (Yellow, blinks at 8 Hz)	System is shutting down (Shutting Down after *SWAP* button pressed)
		On (Red, blinks at 8 Hz)	Malfunction status
		Off	Card is powered off and can be removed.
XENPAK port indicator			

Status indicator:	Link	On (Green)	Network connection on XENPAK transceiver is normal
		Off	No network connection present on XENPAK transceiver
Transmission Indicator	Act	Blinking (Green)	Sending or receiving data

1.4.2.5.3 Front Panel Port Description

EM4700BD-2XG-XENPAK provides 2 XENPAK 10Gb fiber transceiver slots;

Table 1.14 XENPAK port descriptions

Port Type	Specification
XENPAK	● XENPAK-SC transceiver (10GBASE-LR LAN-PHY) (Agilent HFCT-701XB, LAN mode, wavelength 1310nm)： 62.5/125 μm multi-mode fiber (MMF): 300m 9/125 μm single-mode fiber (SMF): 10Km

1.4.2.5.4 Front Panel – Reset Button

The EM4700BD-2XG-XENPAK provides a ***RESET*** button for resetting the board.

1.4.2.5.5 Front Panel – SWAP Button

The EM4700BD-2XG-XENPAK provides a SWAP button for hot swapping the module during operation. Before removing the modules, users should first press the SWAP button. The module will then prepare for a hot-swap and the system operation indicator (RUN) will turn yellow and blink at 8 Hz. When the ***RUN*** indicator is off, the cards are powered off and can be removed.

1.4.3 EM4704BD-AC

ES4704BD uses 1 +1 redundant power supplies. Each of them may serve as a standby power supply for another. Under normal operation conditions, the two power supply modules concurrently operate and each of them bears half of the loads. If one of the power supply modules fails to work or its switch is off, its alarming indicator will be on. At the same time, another power supply becomes responsible for the power supply of the whole switch. When the failure power supply module returns to normal state or its switch is turned on, the alarming indicator will be off.

The power supply modules are installed on the upper part of the machine chassis, and are connected with the backplane of the switch through specific interfaces. The two power supply modules are fixed on the machine chassis with two screws. Each power supply module has one switch. Under normal operation conditions, two switches shall be turned on. For changing power supply modules, it is not necessary to open the chassis. You may turn off the switches of corresponding power supply modules and screwing off the fixing screws for changing the modules.

1.4.3.1 EM4704BD-AC (Alternating Current Power Module)

When powered by AC inputs, the AC power module EM4704BD-AC and corresponding AC distribution box should be used in the ES4704BD. The input voltage of the EM4704BD-AC is 200V/264 VAC, with ranges between 200 ~ 264 VAC and frequency between 50 ~ 60 Hz, the maximum output power is 300W.

1.4.3.2 Power module Front Panel

The front panel of EM4704BD-AC is equipped with power supply switches, power supply indicators as well as ventilating and cooling port and a handle for inserting and pulling out the modules.

The Front Panel view is shown below:

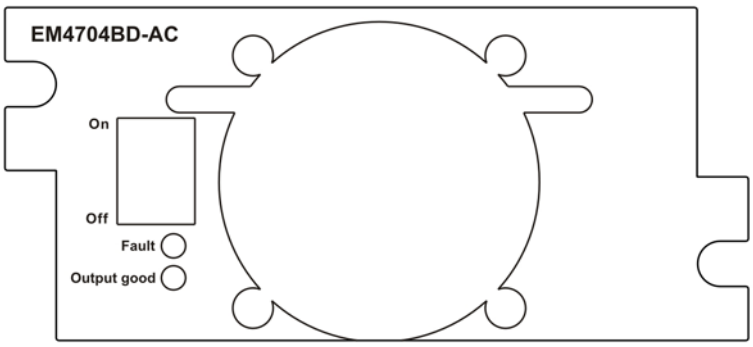


Fig 1-9 EM4704BD-AC Front Panel View

1.4.3.3 LED

The LED description of EM4704BD-AC is as follows

Table 1.15 The Description of EM4704BD-AC LED

LED	Panel Label	Status	Description
Output LED	Output Good	On Green	Power Module Output Status is okay
		Off	Power Module has no output
Abort LED	Fault	On Yellow	Faulty Power Module /Not turning-on The Output Switch
		Off	Power Module Working Fine

1.4.3.4 Switch of power supply for front panel

EM4704BD-AC provides a power supply for controlling the power output of control module. Under normal operation conditions, the switches for power supply modules shall be turned on concurrently. When the switch of one power supply module is turned on and another is turned off, the FAULT indicator of the module will be on to suggest the users to turn on the switch so as to utilize 1+1 redundant backup.

1.4.4 Power Distribution Box

There is a special A.C. distribution box on the backboard of ES4704BD switch.

In generally, the enterprises users usually ask for the 200~264VAC access. The panel of A.C. distribution box is equipped with a 200~264VAC socket for provide power supply to the equipment. At the same time, it provides power supply to the two power supply modules. After the D.C. output is disposed on the backplane, it provides power supply to the modules and fan tray. The lower part of the power supply socket is equipped with a locking ring, which is used to fix the power supply lines to prevent unexpected disconnection and make the wiring more convenient. The distribution box is equipped with a grounding terminal at its lower right part, which is used for grounding the switch..

1.4.5 System Backplane

The system board of ES4704BD is located inside the switch, providing interconnectivity in the high speed data links between management switching modules, network interface modules and between all management and control signals of various cards. A backplane has been installed in the unit chassis. The backplane provides the following functions:

- Provides communication channel for cards to achieve interconnectivity of various signals
- The backplane is powerless
- Supports the hot-swapping of various cards
- Supports Mainboard Master-Slave swap
- Auto identification of all slots
- Distributed power supplies
- Introduction of monitoring signals for fans and power supplies

1.4.6 Fan Tray

Three fan assemblies (EM4704BD-FAN) can be configured in the ES4704BD, and installed in a horizontal configuration into the fan module slots in the switch's upper front panel. The three fan assemblies cover the entire board area, ensuring sufficient ventilation for the devices, hence enhancing the stability of devices even under high temperature environments. Each fan assembly consists of 2 axial fans, which are protected by the fan tray to prevent bodily injury. Please note that the fan blades still spin at a high speed when disconnected from the device during operation, to avoid bodily injury ***do not*** touch the spinning blades.

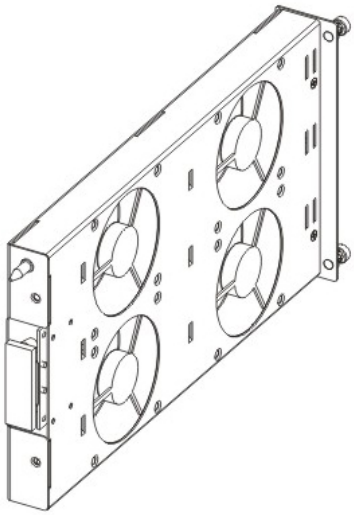


Fig 1-10 EM4704BD-FAN Outlook

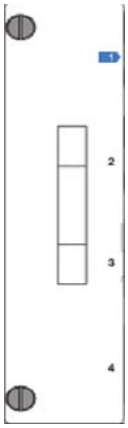


Fig 1-11 EM4704BD-FAN Front Panel View

1.4.7 Dust Gauze

The ES4704BD's dust gauze lies under the board rack and prevents large particles in the air from entering the switch. The dust gauze should be inserted from the front of the ES4704BD in a horizontal position.

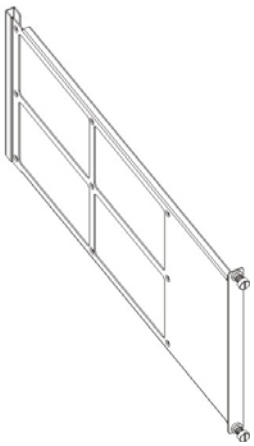


Fig 1-12 Dust Screen Outlook

1.4.8 Rear Panel

The rear panel of the ES4704BD covers the switch backplane. To ensure safe operation of the switch, please ***do not*** open the rear panel. There are two reversible handles on the rear panel, they are used only for the installation and removal of the rear panel. Never lift or move the switch with these handles! The rear panel is shown below:

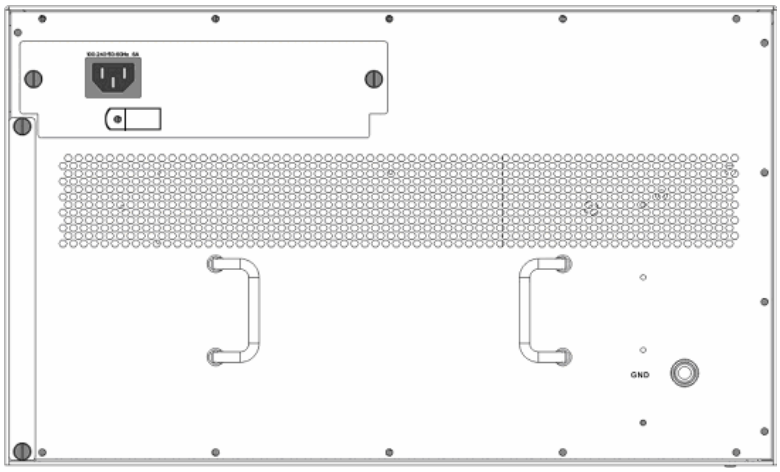


Fig 1-13 Rear Panel View

1.4.9 Side Panels

There are several rows of ventilation openings in the left and right sides of the switch, as shown above.

Please do not block the ventilation openings and ensure that enough clearance is left on both sides of the switch for air circulation. Failure to do so can cause the chassis to overheat and the system to fail, or damage to components.

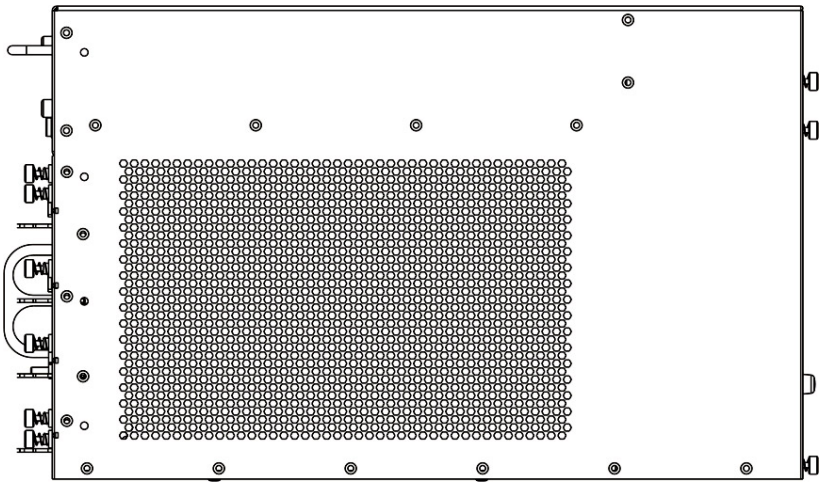


Fig 1-14 Side Panel View

1.5 System Features

Table 1.16 ES4704BD System Features

SDRAM	128MB
FLASH	32MB
Status indicator:	Port: Traffic, LINK General: Power status, system status, hot-swap indicator
Weight	30KG (Max full configuration weight)
Physical Dimensions	445mm x266mm x421mm (W x H x D)
Relative humidity	10% ~ 90% with no condensing
Operating Temperature	0°C ~ 40°C
Power Supplies	Nominal Input Voltage AC: 200 ~ 264 VAC, 50 ~ 60Hz (supporting 1+1 redundant backup of power modules)
Power Consumption	≤ 300 W
Forwarding Mode	Store-and-forward

The ES4704BD Switch system features are described in the table below.

Table 1.17 ES4704BD System Features

Property	**Specification**
Basic Configuration	4 slots
Hot swap	Yes
Failover design	Core part redundant hot swapping
	Power supplies redundant hot swappable
Processor	MPC8245 266MHZ

Chapter 2 Hardware Installation

2.1 Safety Information

During the installation and use of the ES4704BD Switch, please follow the safety guidelines listed below:

Basic Guidelines

1. Disconnect power supplies from the chassis before disassembly or moving the switch.
2. Install the switch in a clean area, ensuring proper temperature and humidity conditions.
3. Keep the device accessories in a safe place.
4. When handling modules, always handle the modules by the edge, avoid contact with integrated components and printed circuits.
5. Prevent electrostatic discharge damage to the integrated components and printed circuits.
6. Keep maintenance tools in a safe place.
7. Do not wear loose clothing that may catch on devices, also remember to fasten ties or scarves and roll up your sleeves.
8. If the environment may cause harm to eyes, be sure to wear a pair of protective goggles.
9. Do not perform any operation that may result in bodily injury or damage to the device.
10. When cleaning the switch, do not use a damp cloth to wipe the switch and never wash the switch with liquids.

Safety Warning

1. Safety warnings appear throughout this publication, referring to operations **that may harm you if performed incorrectly**.
2. Read through the installation instruction carefully before operating the system.
3. Only trained and qualified personnel should be allowed to install, replace, or service the switch.
4. Disconnect power supplies from the chassis before disassembly or moving the switch.
5. The final configuration of the product must abide by all national laws and codes.

Hot Line Work Safety Guidelines

1. Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, watches and bracelets).
2. Metal objects will cause short circuits and damage the device when in contact with both powered items and the ground.
3. An improper connection between the device and power sockets may be hazardous.
4. Only trained and qualified personnel should be allowed to operate and maintain the device.
5. Reading through the installation guidelines before powering on the system.

Notice

! Watch out for potential dangers, e.g. wet floors, ungrounded power lines, and worn power lines.
! Have an emergency switch installed inside the workshop, so that power can be cut off promptly should an accident occur.
! Do not work alone if potential dangers are present.
! On the event of an accident, take the following measures:
1. Power down the system
2. Make emergency calls if required
3. Determine whether the victim requires immediate treatment and take appropriate action
4. If possible, send someone for medical help; otherwise, consider the damage and seek help

2.1.1 Site Requirements

The ES4704BD must be used indoors, and have the following requirements:

Ambient temperature: 0 ~ 40℃

Humidity: 10% ~ 90%, non-condensing

The ES4704BD is equipped with a fan assembly for providing the switch with an appropriate level of cooling; you can place the switch on a workbench or rack. Ensure the following:

- The rack or workbench should be well ventilated. For sufficient air circulation, it is recommended to mount the switch on a 19″ standard rack with sufficient spacing. Air conditioning is recommended in areas with high temperatures in the summer.
- To cool the internal circuits, the switch comes with internal fan assemblies. To maintain proper air circulation through the switch chassis, we recommend that you maintain a minimum 100mm separation between the chassis air intake or the chassis air exhaust and any walls. Make sure that all air intakes and exhausts on the system remain unobstructed. Do not stack heavy items on the switch.
- Make sure the rack or workbench are strong enough to support the weight of a fully configured switch.
- Make sure the rack or workbench is well grounded; if the workbench is not grounded, it should be placed near a grounding conductor to provide easy ground connection for the switch.

2.1.2 Temperature and Humidity Requirements

To maximize the switch's performance and lifespan, the site should maintain a desirable temperature and humidity. High-humidity conditions can cause electrical resistance degradation or even electric leakage, degradation of mechanical properties and corrosion of internal components. Extreme low relative humidity may cause the insulation spacer to contract, making the fastening screw insecure. Furthermore, in dry environments, static electricity is liable to be produced and cause harm to internal circuits. Temperature extremes can cause reduced reliability and premature aging of insulation materials, thus reducing the switch's working lifespan. The recommended temperature and humidity are shown below:

Temperature:		Relative humidity	
Long term condition	Short term condition	Long term condition	Short term condition
15 ~ 30°C	0 ~ 40°C	40～65%	10～90%

Notice

A sample of ambient temperature and humidity should be taken at 1.5m above the floor and 0.4m in front of the switch rack, with no protective panel covering the front and rear of the rack.

Short term working conditions refer to a maximum of 48 hours of continued operation and an annual cumulative total of less than 15 days.

Formidable operation conditions refers to the ambient temperature and relative humidity value that may occur during an air-conditioning system failure, and normal operation conditions should be recovered within 5 hours.

2.1.3 Dust and Particles

Dust is harmful to the safe operation of the ES4704BD. Dust can lead to electrostatic adherence, especially likely under low relative humidity, causing poor contact of metal connectors or contacts. Electrostatic adherence will result in not only reduced product lifespan, but also increased chance of communication failures. The recommended values for dust content and particle diameter in the site are shown below:

Max. Diameter (μm)	0.5	1	3	5
Max. Density (particles/m³)	1.4×10^7	7×10^5	2.4×10^5	1.3×10^5

In addition, salt, acid and sulfide in the air are also harmful to the switch. Such harmful gases will aggravate metal corrosion and the aging of some parts. The chosen site should avoid harmful gases, such as SO_2, H_2S, NO_2, NH_3 and Cl_2, etc. The table below details the threshold values.

Gas	Average (mg/m³)	Max (mg/m³)
SO_2	0.2	1.5
H_2S	0.006	0.03
NO_2	0.04	0.15
NH_3	0.05	0.15
Cl_2	0.01	0.3

2.1.4 Preventing Electrostatic Discharge Damage

Static electric discharges can cause damage to internal circuits, even the entire switch. Follow these guidelines for preventing ESD damage:

1. Ensure proper earth grounding of the device
2. Perform regular cleaning to reduce dust
3. Maintain proper temperature and humidity
4. Always wear an ESD wrist strap and antistatic uniform when in contact with circuit boards

2.1.5 Anti-interference Requirements

All sources of interference, whether from the device/system itself or the outside environment, will affect operations in various ways, such as capacitive coupling, inductive coupling, electromagnetic radiation, common impedance (including the grounding system) and cables/lines (power cables, signal lines, and output lines). The following should be noted:

1. Precautions should be taken to prevent power source interruptions
2. Provide the system with a dedicated grounding, rather than sharing the grounding with electronic equipment or lightning protection devices
3. Keep away from high power radio transmitters, radar transmitters, and high frequency strong circuit devices
4. Provide electromagnetic shielding if necessary

2.1.6 Rack Configuration

The dimensions of the ES4704BD are designed to be mounted on a standard 6" rack, the dimensions are 445mm x 266mm x 421mm (W x H x D). Please ensure good ventilation for the rack.

- Every device in the rack will generate heat during operation, therefore vent and fans must be provided for an enclosed rack, and devices should not be stacked closely,.
- When mounting devices in an open rack, care should be taken to prevent the rack frame from obstructing the switch ventilation openings. Be sure to check the positioning of the switch after installation to avoid the aforementioned.

Notice

If a standard 19" rack is not available, the ES4704BD can be placed on a clean level desktop, leave a clearance of 100mm around the switch for ventilation, and do not place anything on top of the switch.

2.1.7 Power Supply Requirements

The ES4704BD is designed to use modular switching power supplies, supporting 1 +1 redundant backup of power modules. The power input specification is shown below:

Nominal Input Voltage

AC: 200 ~ 264 VAC, 50 ~ 60Hz

Total power consumption: ≤300W

Before installing the power modules, please check the power input to ensure proper grounding of the power supply system. The input source for the switch should be reliable and secure, a voltage adaptor can be used if necessary. The building's circuit protection system should include in a fuse or circuit-breaker of no greater than 240V, 10A. It is recommended to use a UPS for more reliable power supply.

⚠ Notice

Improper power supply system grounding, extreme fluctuation of the input source, and transients (or spikes) can result in larger error rate, or even hardware damage.

2.2 Preparing for Installation

After verifying site requirements, please check the contents of the switch container and accessory kit. (If you are concerned that any item is missing or an incorrect item has been supplied, please contact your dealer as soon as possible.)

2.2.1 Checking Switch Hardware Configuration and Accessories

After verifying site requirements, you can now unpack the shipping container to verify the switch configuration and contents of the accessory kit.

A basic configuration ES4704BD should include the following:

ITEM No.	Part name	Number	Memo
1	ES4704BD Ethernet Switch	1	
2	AC cable	3	
3	Serial port cable	1	
4	Grounding cord	1	
5	Chassis hanger	2	
6	Hanger screw	8	
7	Rack screw	8	

8	Manual CD	1	
9	Qualification certificate	1	
10	Warranty card	1	

Note: The above list is subject to change without notice, please use the packing list shipped with the switch as the checklist.

2.2.2 Required Tools and Utilities

Required tools	● cross screwdrivers
	● Flat-blade screwdriver
	● ESD-preventive wrist strap
Connection cables	● Serial port cable
	● Multi-mode fiber cable
	● Single-mode fiber cable
	● Category 5 cable with RJ-45 connector

2.3 Hardware Installation

The installation of the ES4704BD includes the following:

- ☞ Switch mounting
  - ■ Desktop installation
  - ■ Rack-mounting the switch
- ☞ Switch grounding
- ☞ Cards and modules installation
- ☞ Connecting to the Console
  - ■ Connecting to the Console port
- ☞ Connecting to the Management Port
  - ■ Connecting to the Ethernet port
- ☞ SFP transceiver installation
  - ■ Install the SFP transceiver in the SFP slot
- ☞ XENPAK transceiver installation
  - ■ Install the XENPAK transceiver in the XENPAK slot
  - ■ Copper Cable/Fiber cable connection
  - ■ Ethernet cable connection
  - ■ Fiber cable connection
- ☞ Power supply connection

2.3.1 Switch Installation

2.3.1.1 Desktop installation

- **Note:**
  - Choose a smooth level workbench
  - Verify that the workbench is strong enough to support the ES4704BD's fully configured weight
  - Plan a good position for your ES4704BD that is easy to operate and has an appropriate power source and grounding point.
  - Place the ES4704BD safely on the workbench, avoid obstructions on any side of the switch.

⚠ Notice

To avoid damage, do not place any weight on the switch.

2.3.1.2 Rack-mounting ES4704BD

- **Note:**

  Before mounting the ES4704BD into the rack, verify that the mounting positions of the rack are correct. Preposition of the mounting points may result in inadequate spacing between the switch front panel and the rack front door, and the rack front door may be unable to be closed with cables and fiber cables connected. Please keep a 10 mm spacing between the switch front panel and the rack front door.

  Verify the following before installation: the rack is stably positioned; all modules inside the chassis are fully installed; no obstructions are present inside or around the rack; the switch is situated near the rack for ease of installation.

- **Installation Steps**

  Step 1: Attach the 2 hangers on the ES4704BD with screws provided in the accessory kit.

  Be sure to attach the hangers in the correct direction, otherwise the switch will not be able to mount into a standard rack.

  Note that the hangers are not weight bearing. They are used to fasten the switch. The mounting Shelf or sliding rails (bolt to the rack) will support the switch.

  The figure below shows the steps for mounting the hangers:

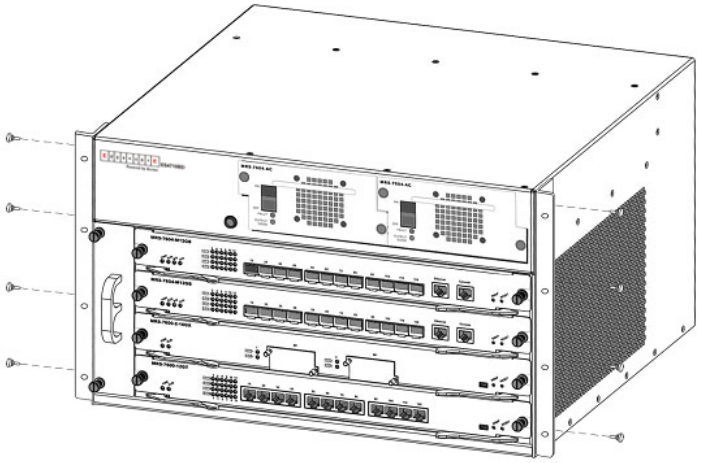


Fig 2-1 Installing ES4704BD Switch Hangers

Step 2: Put the hanger-mounted switch smoothly into a standard 6" rack.

Because of the size and weight of a ES4704BD, 2 people are required to complete the installation. With a person standing on each side of the chassis, grasp the chassis handle in the lower side panel with one hand, and use the other hand near the top of the chassis for balance. Slowly lift the chassis in unison and carry it to the rack. Lift the ES4704BD to a position a little higher than the mounting shelf or sliding rails, resting the chassis on the shelf/rails, and then carefully slide the chassis into the rack. Be sure to align the hangers and mounting holes in the rack column.

Step 3: Fasten the ES4704BD to the rack with the screws provided.

Bolt the hangers to the matching holes in the rack column with the screws provided. Be sure to tighten the screws smoothly. The ES4704BD should now be securely attached to the equipment rack.

The procedure is shown below:

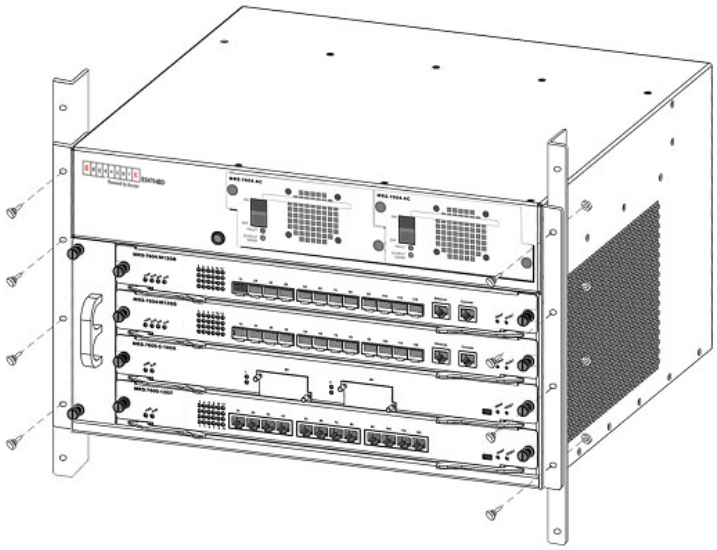


Fig2-2 Rack-mounting ES4704BD

2.3.1.3 Wearing an ESD Wrist Strap

An ESD Wrist Strap must be worn during the installation of the switch. To prevent any damage

occurring to the device, avoid contact between the printed circuit boards and your clothing. Avoid bodily contact with components on the circuit boards if possible.

To wear an ESD Wrist Strap:
Step 1: place your hand into the ESD wrist strap
Step 2: tighten the fastener and ensure that it makes maximum contact with the skin
Step 3: Insert the equipment end of the strap into the antistatic socket (indicated by an ESD symbol) in the switch front panel

2.3.2 Switch grounding

A good grounding system is the groundwork for the smooth and safe operation of the ES4704BD, and an excellent way to prevent lightning strikes and resistance interference. Please follow the switch grounding specification instructions, verify the installation site's grounding condition and ensure proper grounding accordingly.

- **Proper grounding**

When using an AC power source, the device must be grounded with the green and yellow ground cables, otherwise, shock hazards may occur when insulation resistance between the internal power supply and the chassis degrades.

- **Lightning protection grounding**

The lightning protection system is an independent system consisting of a lightning rod, conductor and connection joint with the grounding system. The grounding system usually is shared with the power reference grounding and green and yellow ground cable grounding. Lightning protection grounding is a building requirement, not a specific requirement of the switch.

- **Electromagnetic compliance grounding**

This refers to the grounding to comply with switch electromagnetic compatibility requirements, including shielded grounding, filter grounds, noise, and interference control and level reference. The overall grounding requirements are the sum total of the above. Ground resistance value should be less than 1 ohm.

The ES4704BD provides chassis grounding post in the lower rear chassis, marked as "GND". Chassis protection grounding should be properly connected to the rack grounding connector

The ground cabling procedures are listed below:

Step 1: remove the nuts from the rear chassis grounding posts

Step 2: wrap one end of the green and yellow grounding cable to the grounding posts

Step 3: attach the grounding post nut and tighten well

Step 4: attach the other end of the grounding cable to the rack grounding connector

Note:

- The grounding cable should be made of a good conductor, and the diameter should be

determined by the possible maximum current that may pass through.

- Bare conductor cabling is forbidden.
- Ground resistance value: the combined grounding resistance should be less than 1 ohm.

2.3.3 Card and module installation

The ES4704BD is a rack-mounting device, various cards and modules are available.

Basic configuration: chassis, power supply modules (optional 1 +1 redundant), system backplane, fan tray, dust gauze, distribution box. The above parts have been mounted upon shipment, please verify they are properly locked before installation.

2.3.3.1 Removing and Installing the Cards

The installation procedure is the same for all cards, as shown below:

Step 1: Power down the switch (Hot-swapping is supported by optional cards for the switch. However, for better convenience, it is recommended to power down the switch before installing the cards, if no module in the switch is running.)

Step 2: Ensure proper grounding of the switch

Step 3: Put on an ESD wrist strap before contact with the switch circuit, and make sure the ESD wrist strap is connected securely to the ESD connector in the switch's front panel.

Step 4: Loosen the panel fasteners locking back plate counterclockwise and remove the back plate.

Step 5: Insert the optional module into the slot, you can use the metal handle on the front plate of the module to ensure good contact. Then lock the module with panel fasteners in the front plate.

2.3.3.2 Removing and installing the Dust Gauze

Dust gauze is provided in the right section of the ES4704BD, which can be installed and removed from the back of the switch. The dust gauze is meant to prevent large debris or particles in the air from being ingested into the switch. Please perform cleaning on a regular basis according to the site conditions.

- Loosen the 2 panel fasteners in the dust gauze
- Draw the dust gauze out smoothly by holding the 2 screws
- Clean the dust gauze with a brush (never wash with any liquid)
- Insert the gauze back to its original position in the switch
- Tighten the panel fasteners.

Note: The dust gauze is installed on switch chassis shipment.

The installation and removal of the dust gauze is shown below:

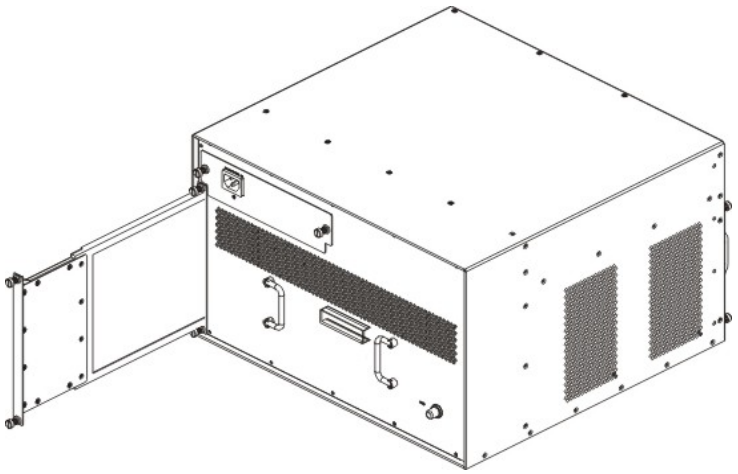


Fig2-3 Installation and removal of the dust gauze

2.3.3.3 Removing and Installing the Fan Tray

The ES4704BD has two fan trays in the left section of the switch, and can be serviced from the front. The installation and removal of the fan tray is relatively simple. To install, just hold the fan tray in the correct direction, align with the corresponding slot and push to secure. Tighten the panel fasteners in the font panel. Upon removal, first loosen the 2 screws in the front panel of the fan tray, hold the handle in the front panel of fan tray with your middle and ring fingers, press the locker slightly down, and the fan tray can be drawn out smoothly.

Note: The fan trays are installed on switch chassis shipment.

The installation and removal of a fan tray is shown below:

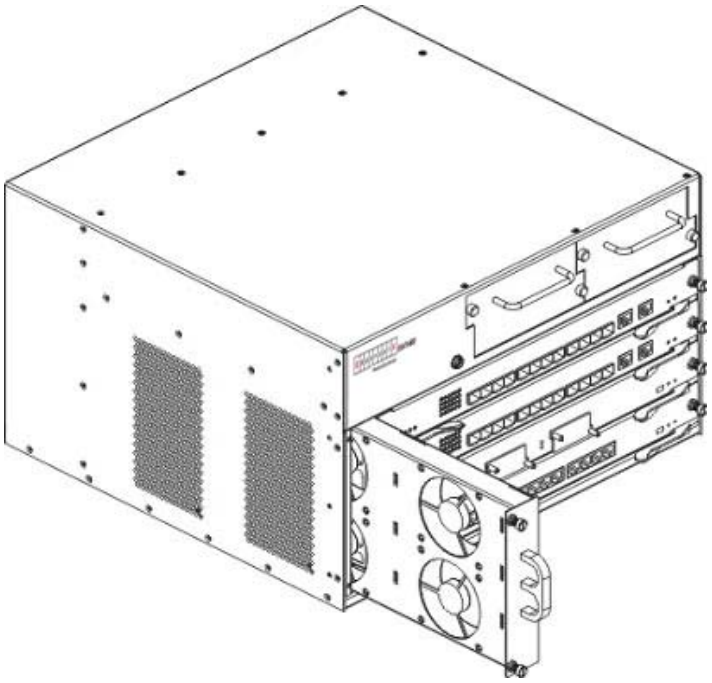


Fig2-4 The installation and removal of a fan tray

2.3.3.4 Removing and Installing Power Supply Modules

The ES4704BD employs a 1 +1 redundant power supply module combination, all two modules will work during normal operation. In case one module fails, it can be replaced while the system is operating without presenting an electrical hazard or damage to the system. The procedures are provided below:

Step 1: First, turn off the switch in the front panel of the power supply module to be replaced

Step 2: Loosen the 2 panel fasteners in the front panel of the power supply module to be replaced by turning the screwdriver counter clockwise

Step 3: Hold the handle in the upper front panel of the power supply module, and draw out the power supply module firmly and smoothly

Step 4: Turn off the switch in the front panel of the new power supply module, use the new power supply module and replace the failed module . Tighten the panel fasteners in the font panel

Step 5: Turn on the switch in the front panel of the power supply module, successful replacement will be indicated by the green OUTPUT GOOD indicator on the front panel of the power supply module being illuminated and by the yellow Fail indicator not illuminating.

Installation of a power supply module is shown below:

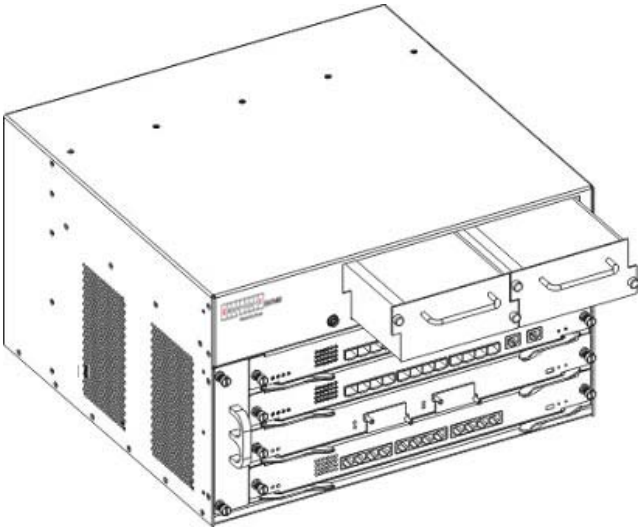


Fig 2-5 The installation and removal of power supply modules

2.3.4 Connecting to the console

The ES4704BD provides a RJ-45 port as the local console. Users can configure the switch through a character terminal (usually a PC) with RS-232 ports. The connection procedures are listed below:

Step 1: Find a character terminal or a PC with a RS-232 serial port.

Step 2: Connect the RS-232 serial port of character terminal to the configuration port of the switch, ensuring at least one of them is powered down.

⚠ Notice

Upon connection, please verify the sign above the port to avoid using the wrong port.

2.3.5 Connecting to the Management Port

The EM4704BD-M12GX-SFP and EM4704BD-M24TX4GC provides a RJ-45 (female) Ethernet port. Users can connect to this administration port through a backend host with Ethernet interface for program loading, or use this port to connect to remote devices (e.g., an administrative workstation) for remote administration. The connection procedure is listed below:

- Connecting to a back-end PC
  - Step 1: Find a PC with Ethernet Interface
  - Step 2: Connect the PC to the RJ-45 Ethernet port of the switch with a twisted-pair crossover cable
- Remote Administration of the device
  - Step 1: Connect the administrative Ethernet port in the main controlling board to a Hub with a standard network cable
  - Step 2: Connect the Hub to an administrative workstation in the local area network.
  - Or,
  - Step 1: Connect the administrative Ethernet port in the main controlling board to a router with a crossover network cable
  - Step 2: Connect the router to an administrative workstation in the wide area network.

2.3.6 SFP transceiver installation

In the ES4704BD, each line card with a 1000BASE fiber interface provides several SFP 1000BASE transceiver slots.

The procedure for installing the SFP 1000BASE fiber transceiver is shown below:

Step 1: Put on a ESD wrist strap (or antistatic gloves)

Step 2: Insert the SFP transceiver onto the guide rail inside the 1000BASE fiber interface line card Do not put the SFP transceiver up-side-down.

Step 3: Push the SFP transceiver along the guide rail gently until you feel the transceiver snap into place at the bottom of the line card.

Note: the SFP 1000BASE fiber transceiver is hot swappable.

Notice

Do not stare directly at the 2 fiber bore in the SFP 1000Base fiber transceiver when the switch is in operation. The laser may hurt your eyes.

2.3.7 XENPAK transceiver installation

In the ES4704BD, Each EM4700BD-2XG-XENPAK line card provides 2 XENPAK 10GB fiber transceiver slots. The procedure for installing the XENPAK 10GB fiber transceiver is shown below:

Step 1: Put on an ESD wrist strap (or antistatic gloves)

Step 2: Insert the XENPAK transceiver onto the guide rail inside the 10GB line card. Do not put the XENPAK transceiver up-side-down.

Step 3: Push the XENPAK transceiver along the guide rail gently until it comes into contact with the front panel of the 10GB line card.

Step 4: Tighten (clockwise) the panel fasteners in the front of XENPAK transceiver until fastened to the front panel of the 10GB line card.

Note: the XENPAK 10GB fiber transceiver is hot swappable

Notice

Do not stare directly at the 2 fiber bore in the XENPAK 10GB fiber transceiver when the switch is in operation. The laser may hurt your eyes.

2.3.8 Copper Cable/Fiber Cable Connection

Ethernet cable connection:

Step 1: Insert one end of the Ethernet cable into the RJ-45 Ethernet port in the switch copper cable line card

Step 2: Insert the other end of the Ethernet cable into the RJ-45 Ethernet port of the other device

Step 3: Check all status indicators for the corresponding ports, a lighted LINK indicates the link has been established, otherwise the link is not ready and the cable should be examined

Notice

Upon connection, please verify the sign above the port to avoid use of other ports, which might damage to the modules or the switch.

The connection procedure for fibers are listed below:

Step 1: Remove the protective dust plug from the SFP/XENPAK fiber transceiver bore; take out the fiber cable and remove the protective cap from one end of the fiber cable. Keep the fiber end clean and neat.

Step 2: Immediately attach the end of the fiber cable to the SFP/XENPAK transceiver, and the other end to the transceiver of the corresponding device. Note: Upon connection, the SFP/XENPAK transceiver's TX port should be connected to the RX port of the corresponding device, and vice versa.

Step 3: Check the fiber port status indicator, a lighted LINK indicates that the link has been established, otherwise the link is not ready and should be examined.

Notice

Upon connection, please verify the sign above the port to avoid using other ports, which might damage the transceiver or the other ports.

When connecting the other device through fiber cable to the switch, the output power of the fiber must not exceed the maximum received power of the corresponding modules, otherwise, it will damage the switch. Do not stare at the fiber bore when the switch is in operation to avoid harm.

2.3.9 Power supply connection

Connection procedures for the AC power supply module are described below:

Step 1: Insert one end of electrical line into the power supply socket and another end into the corresponding socket of the switch; when connecting electrical lines, it shall be confirmed that the power supply modules are power off.

Step 2: It shall be examined whether or not the fan on the power supply module operates normally. If the fan fails to operate, please examine whether the power supply socket is power on and whether the power supply module are inserted and locked properly.

Step 3: Turn on the power supply modules (if there are two power supply modules, both of them shall be turned on.), and examine whether or not the indicator of the indicator of the front panel is normal. If the OUTPUT GOOD indicator fails to be on, please turn off the power supply without delay and examine the status of power supply and each inserting plate.

⚠ Notice

If the Power OK indicator does not illuminate after repeating the above steps, please contact the dealer. Do not open the switch chassis by yourself. Please contact the dealer in the case of any failure.

Chapter 3 Setup Configuration

Setup configuration refers to the initial operation of the switch after the user purchases the switch. For first-time users of the ES4704BD, this chapter provides a very practical instruction. When using CLI (command line interface), the user can type *setup* under admin mode to enter the Setup configuration interface.

3.1 Setup Configuration

Setup configuration is done via menu selections, in which the switch's hostname, Vlan1 interface, Telnet service and SNMP can be configured.

3.1.1 Main Setup Menu

Before entry into the main menu, the following screen will be displayed to prompt the user to select a preferred interface language. English users should choose "0" to enter the English interface, while Chinese users can choose "1" to view the interface in Chinese.

Please select language:

[0]:English

[1]:中文

Selection(0|1)[0]:

The main Setup configuration menu is listed below:

Configure menu

[0]: Config hostname

[1]: Config interface-Vlan1

[2]: Config telnet-server

[3]: Config web-server

[4]: Config SNMP

[5]: Exit setup configuration without saving

[6]: Exit setup configuration after saving

Selection number:

The corresponding menu items in Chinese are:

配置菜单

[0]:配置交换机主机名

[1]:配置 Vlan1 的接口

[2]:配置交换机 Telnet 服务器

[3]:配置交换机 Web 服务器

[4]:配置 SNMP

[5]:退出 setup 模式不保存配置结果

[6]:退出 setup 模式保存配置结果

选择序号:

3.1.2 Setup Submenu

3.1.2.1 Configuring switch hostname

Select “0” in the Setup main menu and press Enter, the following screen will appear:

Please input the host name[ES4704BD]:

The corresponding prompt in Chinese is:

请输入交换机主机名[ES4704BD]:

Note: the hostname should be less than 30 characters. If the user presses Enter without input, the hostname will be set to default “ES4704BD”.

3.1.2.2 Configuring Vlan1 Interface

Select “1” in the Setup main menu and press Enter to start configuring the Vlan1 interface:

Config Interface-Vlan1

[0]: Config interface-Vlan1 IP address

[1]: Config interface-Vlan1 status

[2]: Exit

Selection number:

The corresponding prompt in Chinese is:

配置 Vlan1 接口

[0]: 配置 Vlan1 接口的 IP 地址

[1]: 配置 Vlan1 接口的状态

[2]: 返回上一级菜单

选择序号:

Select “0” in the Vlan1 interface configuration menu and press Enter, the following screen will appear:

Please input interface-Vlan1 IP address (A.B.C.D):

The corresponding prompt in Chinese is:

请输入 Vlan1 接口的 IP 地址(A.B.C.D):

When the user enters a valid IP address for Vlan1 interface and presses Enter, the following screen will appear:

Please input interface-Vlan1 mask [255.255.255.0]:

The corresponding prompt in Chinese is:

请输入 Vlan1 接口的子网掩码 [255.255.255.0]:

The system will show default mask of the Vlan1 interface to 255.255.255.0. The user can configure the IP address and mask according to their own network conditions. After configuration, the menu will return to the Vlan1 interface configuration section.

Select “1” in the Vlan1 interface configuration menu and press Enter, the following screen will appear:

Open interface-Vlan1 for remote configuration ? (y/n) [y]:

The corresponding prompt in Chinese is:

是否打开 Vlan1 的接口? (y/n) [y]:

Type “n” and press Enter to disable Vlan1 interface. Type “y” and press Enter, or just press Enter to enable the Vlan1 interface. The Vlan1 interface configuration menu will then appear. Select “2” in the Vlan1 interface configuration menu to return to the Setup main menu.

3.1.2.3 Telnet Server Configuration

Select “2” in the Setup main menu and press Enter to start configuration of the Telnet server, the following will appear:

Configure telnet server

[0]: Add telnet user

[1]: Config telnet server status

[2]: Exit

Selection number:

The corresponding prompt in Chinese is:

配置 Telnet 服务器

[0]: 添加 Telnet 服务器用户

[1]: 配置 Telnet 服务器的状态

[2]: 返回上一级菜单

选择序号:

Select “0” in the Telnet server configuration menu and press Enter, the following screen will appear:

Please input the new telnet user name :

The corresponding prompt in Chinese is:

请输入要添加的 Telnet 用户名:

Note: Valid username length is 1 to 16 characters. When a user enters a valid username and presses Enter, the following screen will appear:

Please input the new telnet user password:

The corresponding prompt in Chinese is:

请输入用户密码:

Note: Valid password length is 1 to 8 characters. After configuring the username and password, the menu will return to the Telnet server configuration section.

Select “1” in the Telnet server configuration menu and press Enter, the following will screen appear:

Enable switch telnet-server or no?(y/n) [y]:

The corresponding prompt in Chinese is:

是否使能交换机 Telnet 服务器?(y/n) [y]:

Type “n” and press Enter to disable Telnet service. Type “y” and press Enter, or just press Enter to

enable Telnet service. The Telnet server configuration menu will then appear.

Select “2” in the Telnet server configuration menu to return to the Setup main menu.

3.1.2.4 Configuring Web Server

Select “3” in the Setup main menu and press Enter to start configuration of the Web server:

Configure web server

[0]: Add web user

[1]: Config web server status

[2]: Exit

Selection number:

The corresponding prompt in Chinese is:

配置 Web 服务器

[0]: 添加 Web 服务器用户

[1]: 配置 Web 服务器的状态

[2]: 返回上一级菜单

选择序号:

Select “0” in the Web server configuration menu and press Enter, the following screen will appear:

Please input the new web user name:

The corresponding prompt in Chinese is:

请输入要添加的 Web 用户名:

Note: valid username length is 1 to 16 characters. When a valid username is entered, press Enter to bring up the following prompt:

Please input the new web user password:

The corresponding prompt in Chinese is:

请输入用户密码:

Note: valid password length is 1 to 8 characters. After configuring the username and password, the menu will return to the Web server configuration section.

Select “1” in the Web server configuration menu and press Enter, the following screen appears:

Enable switch web-server or no?(y/n) [y]:

The corresponding prompt in Chinese is:

是否使能交换机 Web 服务器?(y/n) [y]:

Type “n” and press Enter to disable Web service. Type “y” and press Enter, or just press Enter to enable Web service. The Web server configuration menu will then appear.

Select “2” in the Web server configuration menu to return to the Setup main menu.

3.1.2.5 Configuring SNMP

Select “4” in the Setup main menu and press Enter to start configuring SNMP, the following will appear:

Configure SNMP

[0]: Config SNMP-server read-write community string

[1]: Config SNMP-server read-only community string

[2]: Config traps-host and community string

[3]: Config SNMP-server status

[4]: Config SNMP traps status

[5]: Add SNMP NMS security IP address

[6]: Exit

Selection number:

The corresponding prompt in Chinese is:

配置 SNMP

[0]: 配置 SNMP 读写访问团体字符串

[1]: 配置 SNMP 只读访问团体字符串

[2]: 配置 Traps 主机 IP 地址和团体字符串

[3]: 配置交换机 SNMP 状态

[4]: 配置交换机 Traps 状态

[5]: 添加 SNMP 管理站安全 IP 地址

[6]: 返回上一级菜单

选择序号:

Select “0” in the SNMP configuration menu and press Enter, the following screen will appear:

Please input the read-write access community string[private]:

The corresponding prompt in Chinese is:

请输入 SNMP 读写访问团体字符串[private]:

Note: valid length for a read-write access community string is 1 to 255 characters, the default value is “private”. When a valid read-write access community string has been entered, pressing Enter to returns to the SNMP configuration menu.

Select “1” in the SNMP configuration menu and press Enter, the following screen will appear:

Please input the read-only access community string[public]:

The corresponding prompt in Chinese is:

请输入 SNMP 只读访问团体字符串[public]:

Note: the valid length for a read-only access community string is 1 to 255 characters, the default value is “public”. When a valid read-only access community string is entered, press Enter to return to the SNMP configuration menu.

Select “2” in the SNMP configuration menu and press Enter, the following screen will appear:

Please input traps-host IP address(A.B.C.D):

The corresponding prompt in Chinese is:

请输入接收 Traps 的主机 IP 地址(A.B.C.D):

When users enter a valid IP address for Traps host and press Enter, the following appears:

Please input traps community string[public]:

The corresponding prompt in Chinese is:

请输入通信团体字符串[public]:

Note: valid length for a traps community string is 1 to 255 characters, the default value is “public”. When a valid traps community string has been entered, press Enter to return to the SNMP configuration menu.

Select “3” in the SNMP configuration menu and press Enter, the following screen will appear:

Enable SNMP-server? (y/n) [y]:

The corresponding prompt in Chinese is:

是否使能交换机 SNMP? (y/n) [y]:

Type “n” and press Enter to disable SNMP service. Type “y” and press Enter, or just press Enter to enable SNMP service. The SNMP configuration menu will then appear.

Select “4” in the SNMP configuration menu and press Enter, the following screen will appear:

Enable SNMP-traps ? (y/n) [y]:

The corresponding prompt in Chinese is:

是否使能交换机发送 Traps ? (y/n) [y]:

Type “n” and press Enter to disable SNMP traps. Type “y” and press Enter, or just press Enter to enable SNMP Traps. The SNMP configuration menu will then appear.

Select “5” in the SNMP configuration menu and press Enter, the following screen appears:

Please input the new NMS IP address(A.B.C.D):

The corresponding prompt in Chinese is:

请输入要添加的 SNMP 管理站安全 IP 地址(A.B.C.D):

When a valid secure IP address(es) for SNMP management workstation is entered, press Enter to return to the SNMP configuration menu.

Selecting “6” in the SNMP configuration menu to return to the Setup main menu.

3.1.2.6 Exiting Setup Configuration Mode

Select “5” in the Setup main menu to exit the Setup configuration mode without saving the configurations made.

Selecting “6” in the Setup main menu to exit the Setup configuration mode and save the configurations made. This is equivalent to running the *Write* command. For instance, if under the Setup configuration mode, the user sets a Telnet user, enables Telnet service, and then selects “5” to exit Setup main menu, he/she will be able to configure the switch through Telnet from a terminal.
When exiting the Setup configuration mode, the CLI configuration interface appears. Configuration commands and syntaxes will be described in detail in later chapters.

Chapter 4 Switch Management

4.1 Management Options

After purchasing the switch, the user needs to configure the switch for network management. ES4704BD provides two management options: in-band management and out-of-band management.

4.1.1 Out-of-band Management

Out-of-band management is the management through Console interface. Generally, out-of-band management is used for initial switch configuration, or when in-band management is not available. For instance, the user must assign an IP address to the switch via the Console interface to be able to access the switch through Telnet.

The procedures for management via Console interface are listed below:

Step 1: Setting up the environment:

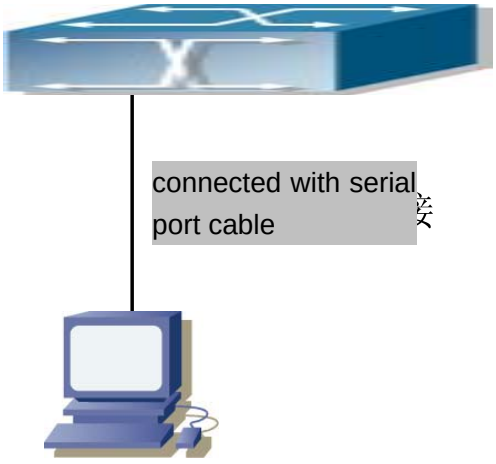


Fig 4-1 ES4704BD Out-of-band Management Configuration Environment

As shown in Fig 4-1, the serial port (RS-232) of a PC is connected to the switch with the serial cable provided. The table below lists all the devices used in the connection.

Device Name	Description
PC	Has functional keyboard, RS-232, and a terminal emulator installed, such as the HyperTerminal which is included in Windows 9x/NT/2000/XP.
Serial port cable	One end attaches to the RS-232 serial port, the other end to the Console port of ES4704BD.
ES4704BD	Functional Console port required.

Step 2 Entering the HyperTerminal.

Open HyperTerminal in Windows after the connection has been established. The example below is based on HyperTerminal that is included in Windows XP.

1) Click Start menu - Programs – Accessories – Communications - HyperTerminal

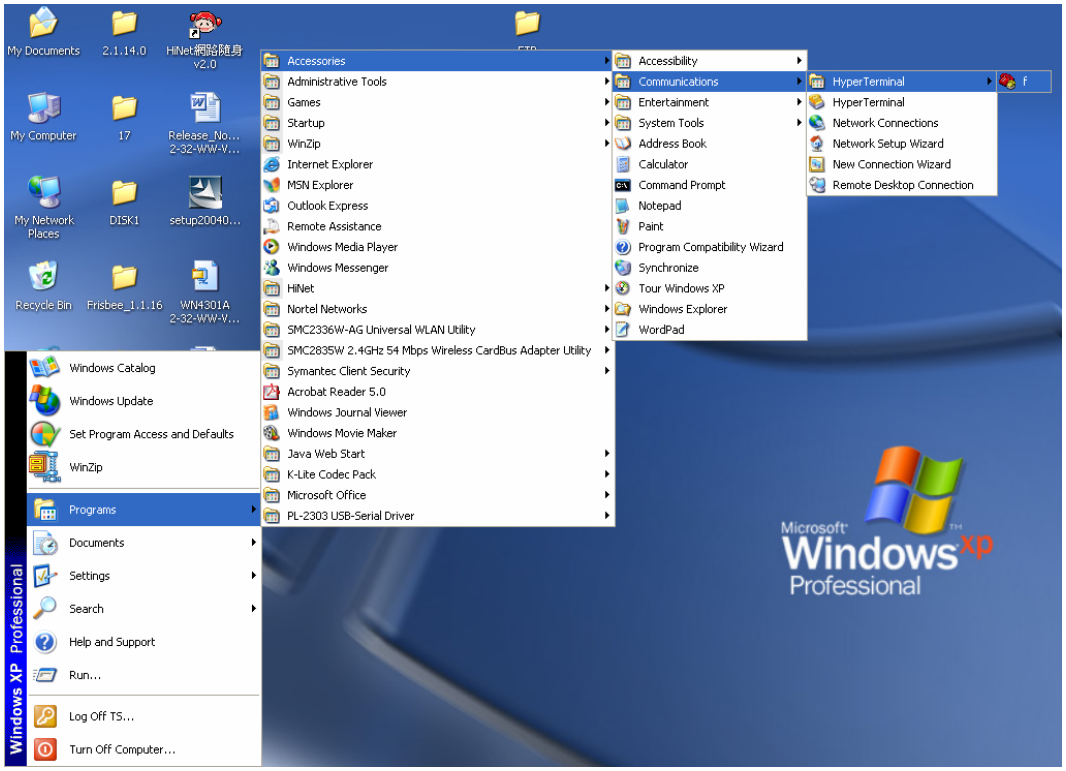


Fig 4-2 Opening HyperTerminal (1)

2) Type a name for opening HyperTerminal, such as “SWITCH”

Fig 4-3 Opening HyperTerminal (2)

3) In the “Connect To” drop-list, select the RS-232 serial port used by the PC, e.g., COM1, and click “OK”.

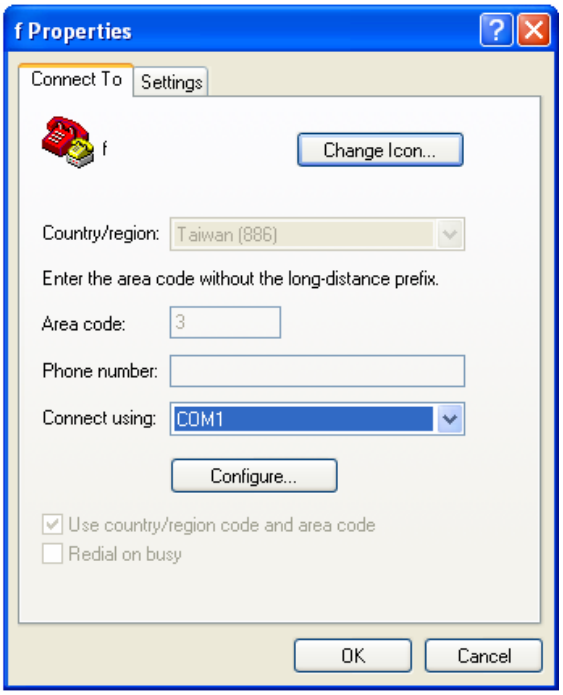


Fig 4-4 Opening HyperTerminal (3)

4) COM1 properties appears, select “9600” for “Baud rate”, “8” for “Data bits”, “none” for “Parity checksum”, “1” for “stop bits” and “none” for “flow control”; or, you can also click “Restore default” and click “OK”.

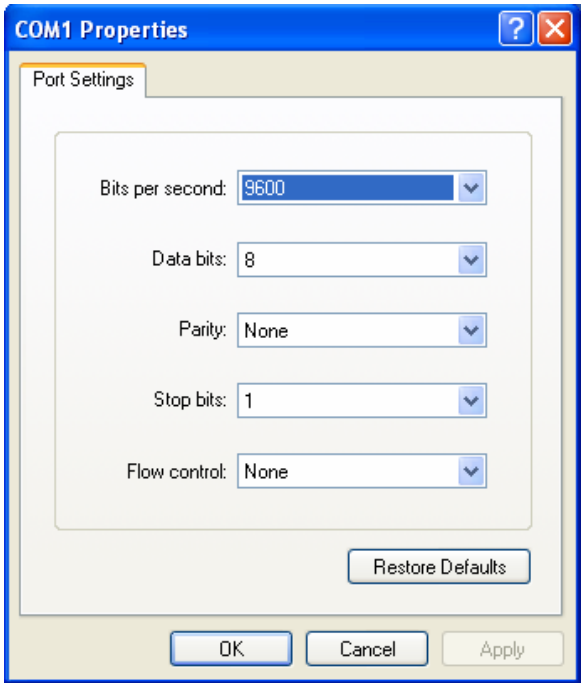


Fig 4-5 Opening HyperTerminal (4)

5)The HyperTerminal window appears.

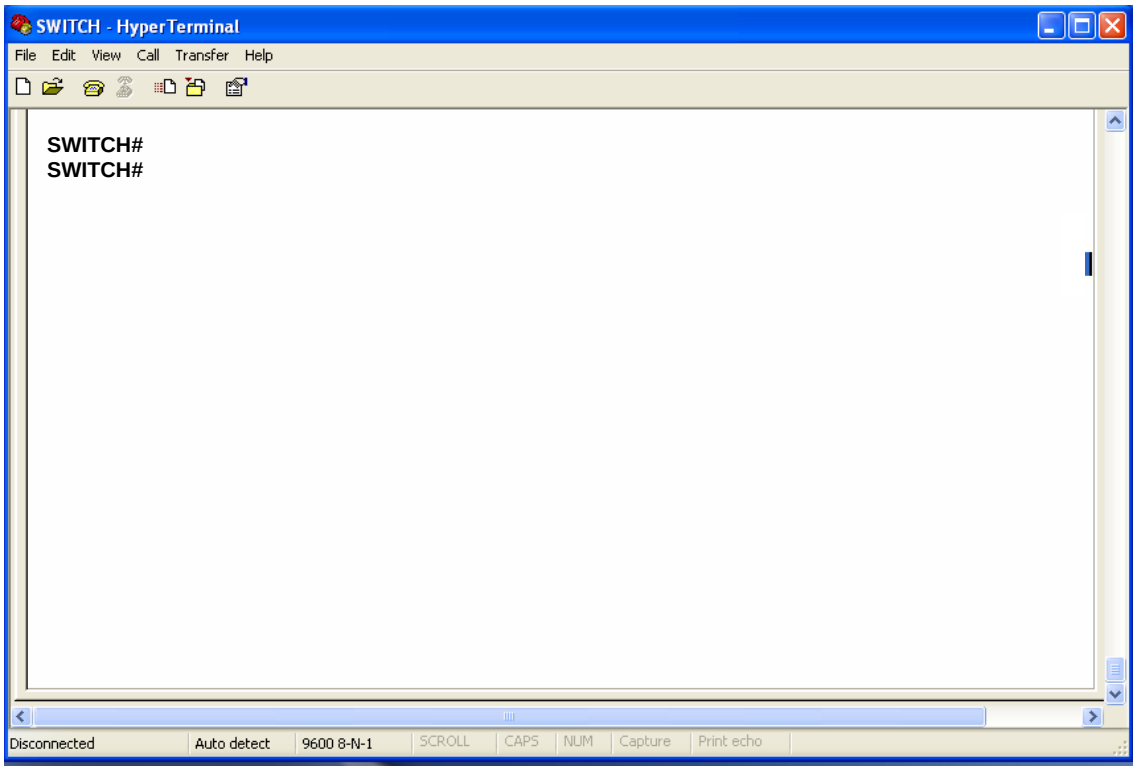


Fig 4-6 Opening HyperTerminal (5)

Step 3 Entering switch CLI interface:

Power on the switch. The following appears in the HyperTerminal windows, this is the CLI configuration mode for ES4704BD.

ES4704BD Management Switch

Copyright (c) 2001-2004 by Edge-Core Networks Limited.
All rights reserved.

Testing RAM...
134,217,728 RAM OK.

Initializing...
Attaching to file system ... done.

Loading nos.img ... done.
Starting at 0x10000...

```
Current time is    WED APR 20 09:37:52 2005

ES4704BD Series Switch Operating System,
Software Packet Version ES4704BD_2.2.10.0
Copyright (C) 2001-2004 by Accton Technology Corp.
http://www.edge-core.com

ES4704BD Switch (MPC8245-266M) processor

ES4704BD>
```

The user can now enter commands to manage the switch. For a detailed description of commands, please refer to the following chapters.

4.1.2 In-band Management

In-band management refers to the management by logging into the switch using Telnet or ECview. ECview is a network management software developed by Edge-Core. In-band management enables management of the switch by devices attached to the switch. In the case when in-band management fails due to switch configuration changes, out-of-band management can be used for configuring and managing the switch.

4.1.2.1 Management via Telnet

To manage the switch with Telnet, the following conditions should be met:

1) Switch has an IP address configured
2) The host's IP address (Telnet client) and the switch's VLAN interface IP address are in the same network segment.
3) If not 2), the Telnet client can connect to an IP address of the switch via other devices, such as a router.

ES4704BD is a Layer 3 switch that can be configured with several IP addresses. The following example assumes the shipment's default status of the switch, only VLAN1 exists in the system.

The following describes the steps for a Telnet client to connect to the switch's VLAN1 interface by Telnet.

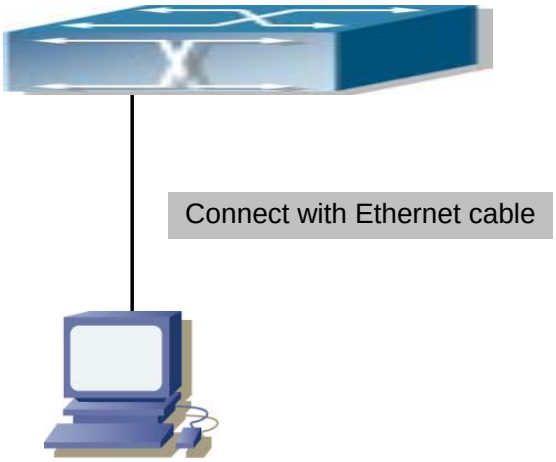


Fig 4-7 Managing the switch by Telnet

Step 1: Configure the IP addresses for the switch and start the Telnet function on the switch.

First, the configuration of the host's IP address should be within the same network segment as the switch's VLAN1 interface IP address. Suppose the switch's VLAN interface IP address is 10.1.128.251/24, then a possible host IP address is 10.1.128.252/24. Run "ping 10.1.128.251" from the host to verify the result, and check for reasons if ping failed.

The IP address configuration commands for VLAN1 interface ES4704BD are listed below. Before in-band management, the switch must be configured with an IP address by out-of-band management (i.e., Console mode), The configuration commands are as follows (All switch configuration prompts are assumed to be "switch" hereafter if not otherwise specified):

```
Switch>
Switch>en
Switch#config
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip address 10.1.128.251 255.255.255.0
Switch(Config-If-Vlan1)#no shutdown
```

At the same time, use the command "telnet-server enable" at console method with global mode to start the function of Telnet server.

The configuration commands：

```
Switch>en
Switch#config
Switch(Config)# telnet-server enable
```

Step 2: Run Telnet Client program.

Run the Telnet client program included in Windows with the specified Telnet target.

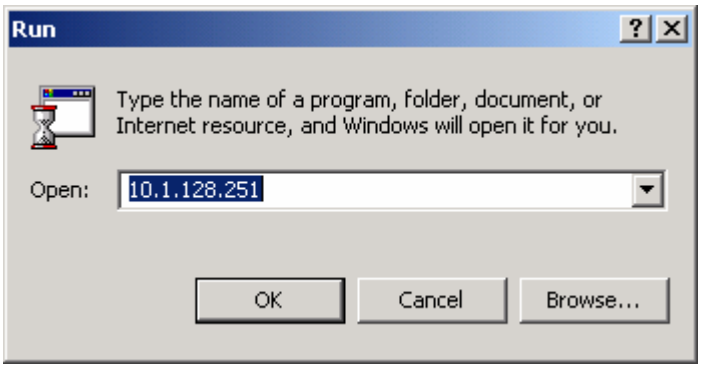


Fig 4-8 Running the Telnet client program included in Windows

Step 3: Log in to the switch

Log in to the Telnet configuration interface. Valid login name and password are required, otherwise the switch will reject Telnet access. This method protects the switch from unauthorized access. If no authorized Telnet user has been configured, nobody can connect to the Telnet CLI configuration interface. As a result, when Telnet is enabled for configuring and managing the switch, username and password for authorized Telnet users must be configured with the following command:

telnet-user <user> password {0|7} <password>

Example: Assume an authorized user in the switch has the username of “test”, and password of “test”, the configuration procedure should like the following:

Switch>en

Switch#config

Switch(Config)#telnet-user test password 0 test

Enter valid login name and password in the Telnet configuration interface, Telnet user will be able to enter the switch’s CLI configuration interface. The commands used in the Telnet CLI interface after login are the same as in the Console interface.

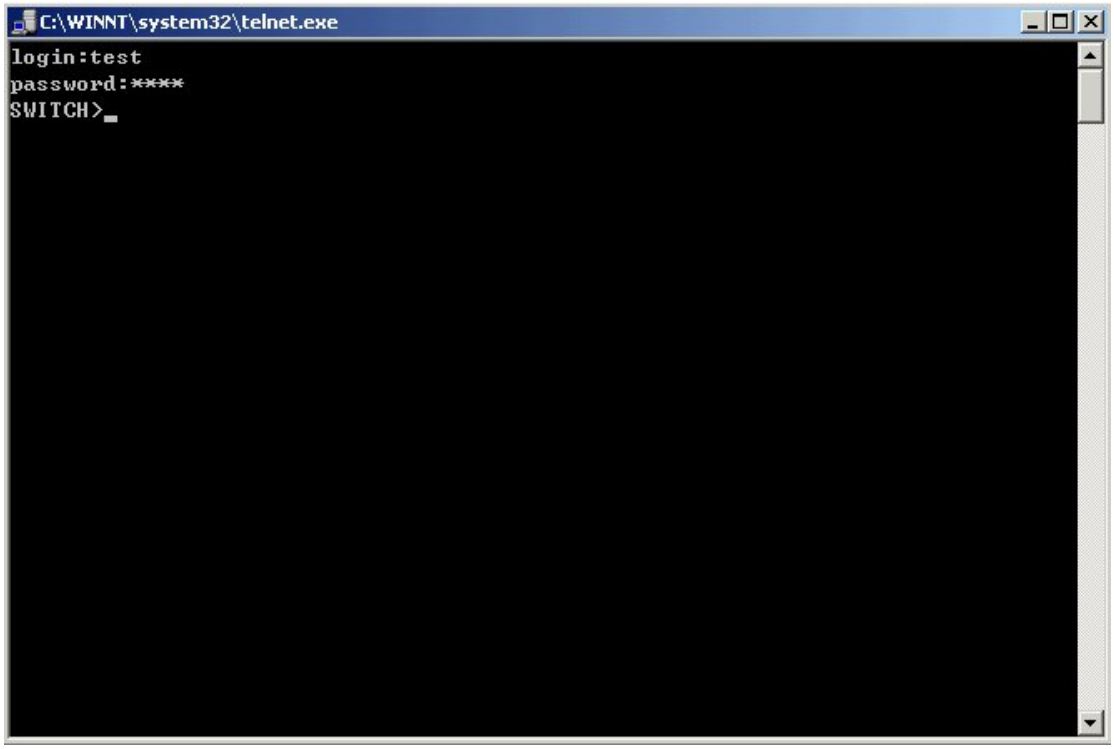


Fig 4-9 Telnet Configuration Interface

4.1.2.2 Managing the Switch through ECview

To manage the switch with ECview, the following conditions should be met:

1) Switch has an IP address configured
2) The host's IP address and the switch's VLAN interface IP address are in the same network segment.
3) If not 2), the client can connect to an IP address of the switch via other devices, such as a router
4) Network management is enabled

The computer hosting ECview should be able to ping the associated IP address of Switch so that ECview will, upon launching, find ES4704BD to perform read/write operations. This manual does not include information about how to manage the switch with ECview, please refer to *ECview User's Guide* for details.

4.2 Management Interface

ES4704BD provides 2 management interface: CLI (Command Line Interface) and ECview software. This manual will focus on the CLI interface, for information about ECview, please refer to *ECview User's Guide*.

4.2.1 CLI Interface

CLI interface is familiar to most users. As aforementioned, out-of-band management and Telnet login are all performed through CLI interface to manage the switch.

CLI Interface is supported by Shell program, which consists of a set of configuration commands. Those commands are categorized according to their functions in switch configuration and management. Each category represents a different configuration mode. The Shell for the switch is described below in Fig 4-10:\

- Configuration Modes
- Configuration Syntax
- Shortcut keys
- Help function
- Input verification
- Fuzzy match support

4.2.1.1 Configuration Modes

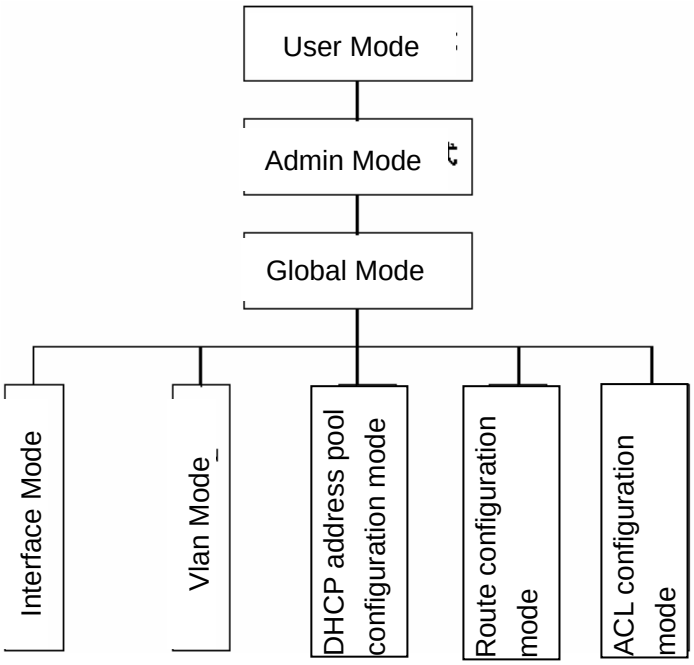


Fig 4-10 Shell Configuration Modes for ES4704BD

4.2.1.1.1 User Mode

On entering the CLI interface, the default is User Mode. The prompt shown is “Switch>”, the symbol “>” is the prompt for User Mode. When the *exit* command is run under Admin Mode, it will return to the User Mode.

Under User Mode, no configuration to the switch is allowed, only clock time and version

information of the switch can be queried.

4.2.1.1.2 Admin Mode

Admin Mode prompt “Switch#” can be entered under the User Mode by running the *enable* command and entering the corresponding admin user password, if set. Or, when the *exit* command is run under Global Mode, it will return to the Admin Mode. ES4704BD also provides the shortcut key sequence "Ctrl+z”, that allows an easy way to exit to Admin Mode from any configuration mode (except User Mode).

Under Admin Mode, the user can query the switch configuration information, connection status and traffic statistics of all ports; and the user can further enter the Global Mode from Admin Mode to modify all configurations of the switch. For this reason, a password must be set for entering Admin mode to prevent unauthorized access and malicious modification to the switch.

4.2.1.1.3 Global Mode

Type the *config* command under Admin Mode to enter the Global Mode, and prompt “Switch(Config)#” will appear. Use the *exit* command under other configuration modes such as Interface Mode or VLAN mode to return to Global Mode.

The user can perform global configuration settings under Global Mode, such as MAC Table, Port Mirroring, VLAN creation, IGMP Snooping start, GVRP and STP, etc. The user can also go further to Interface Mode for configuration of all the interfaces

4.2.1.1.3.1 Interface Mode

Use the *interface* command in Global Mode to enter the interface mode specified. ES4704BD provide three interface type (VLAN interface, Ethernet port, port-channel) and accordingly, the three interface configuration modes. Information is as follows:

Interface Type	Entry	Prompt	Operates	Exit
VLAN Interface	Type ***interface vlan <Vlan-id>*** command under Global Mode.	**Switch(Config-If-VlanX)#**	Configures switch IPs, etc	Use the *exit* command to return to Global Mode.
Ethernet Port	Type ***interface ethernet <interface-list>*** command under Global Mode.	**Switch(Config-ethernetxx)#**	Configures duplex mode, speed, etc. of Ethernet Port.	Use the *exit* command to return to Global Mode.
port-channel	Type ***interface***	**Switch(Config-if-**	Configures	Use the *exit*

	port-channel <port-channel-number> command under Global Mode.	**port-channelx)#**	port-channel related settings such as duplex mode, speed, etc.	command to return to Global Mode.

4.2.1.1.3.2 VLAN Mode

Using the *vlan <vlan-id>* command under Global Mode, you can enter the corresponding VLAN Mode. Under VLAN Mode the user can configure all member ports of the corresponding VLAN. Run the *exit* command to exit the VLAN Mode to Global Mode.

4.2.1.1.3.3 DHCP Address Pool Mode

Type the ***ip dhcp pool <name>*** command under Global Mode to enter the DHCP Address Pool Mode. The prompt "**Switch(Config-<name>-dhcp)#**" will appear. DHCP address pool properties can be configured under DHCP Address Pool Mode. Run the *exit* command to exit the DHCP Address Pool Mode to Global Mode.

4.2.1.1.3.4 Route Mode

Routing Protocol	Entry	Prompt	Operates	Exit
RIP Routing Protocol	Type ***router rip*** command under Global Mode.	**Switch(Config-Router-Rip)#**	Configures RIP protocol parameters.	Use the "*exit*" command to return to Global Mode.
OSPF Routing Protocol	Type ***router ospf*** command under Global Mode.	**Switch(Config-Router-Ospf)#**	Configures OSPF protocol parameters.	Use the "*exit*" command to return to Global Mode.

4.2.1.1.3.5 ACL Mode

ACL type	Entry	Prompt	Operates	Exit
Standard IP ACL Mode	Type ***ip access-list standard*** command under	**Switch(Config-Std-Nacl-a)#**	Configures parameters for Standard IP ACL	Use the "*exit*" command to return to Global Mode.

	Global Mode.		Mode	
Extended IP ACL Mode	Type ***ip access-list extended*** command under Global Mode.	**Switch(Config-Ext-Nacl-b) #**	Configures parameters for Extended IP ACL Mode	Use the "*exit*" command to return to Global Mode.

4.2.1.2 Configuration Syntax

ES4704BD provides various configuration commands. Although all the commands are different, they all abide by the syntax of ES4704BD configuration commands. The general command format of ES4704BD is shown below:

cmdtxt <*variable*> { enum1 | … | enumN } [option]

Conventions: **cmdtxt** in bold font indicates a command keyword; **<*variable*>** indicates a variable parameter; **{enum1 | … | enumN }** indicates a mandatory parameter that should be selected from **enum1~enumN**; and the square bracket ([ ]) in **[option]** indicates an optional parameter. There may be combinations of "< >", "{ }" and "[ ]" in the command line, such as **[<*variable*>]**,**{enum1 <*variable*>| enum2}**, **[option1 [option2]], etc.**

Here are examples for some actual configuration commands:

- **show version**, no parameters required. This is a command with only a keyword and no parameter, just type in the command to run.
- **vlan <*vlan-id*>**, parameter values are required after the keyword.
- **duplex {auto|full|half}**，user can enter *duplex auto, duplex full* or *duplex half* for this command.
- **snmp-server community {ro|rw} <string>**, the followings are possible:
  snmp-server community ro <*string*>
  snmp-server community rw <*string*>

4.2.1.3 Shortcut Key Support

ES4704BD provides several shortcut keys to facilitate user configuration, such as up, down, left, right and Backspace. If the terminal does not recognize Up and Down keys, ctrl+p and ctrl+n can be used instead.

Key(s)	Function
Backspace	Deletes a character before the cursor, and the cursor moves back.
Up "↑"	Shows previous command entered. Up to ten recently entered commands can be shown.
Down "↓"	Shows next command entered. When using the Up key to get previously entered commands, you can use the Down key to return to the next

	command	
Left “←”	The cursor moves one character to the left.	You can use the Left and Right key to modify an entry.
Right “→”	The cursor moves one character to the right.	
Ctrl+p	The same as Up key “↑”.	
Ctrl+n	The same as Down key “↓”.	
Ctrl+b	The same as Left key “←”.	
Ctrl+f	The same as Right key “→”.	
Ctrl+z	Returns to the Admin Mode directly from the other configuration modes (except User Mode).	
Ctrl+c	Breaks the ongoing command process, such as ping or other command execution.	
Tab	When a string for a command or keyword is entered, the Tab can be used to complete the command or keyword if there is no conflict.	

4.2.1.4 Help function

There are two ways in ES4704BD for the user to access help information: the “help” command and the “?”.

Access to Help	Usage and function
Help	Under any command line prompt, type in “help” and press Enter to get a brief description of the associated help system.
“?”	1. Under any command line prompt, enter “?” to get a command list of the current mode and related brief description. 2. Enter a “?” after the command keyword with a embedded space. If the position should be a parameter, a description of that parameter type, scope, etc, will be returned; if the position should be a keyword, then a set of keywords with brief descriptions will be returned; if the output is “<cr>”, then the command is complete, press Enter to run the command. 3. “?” immediately following a string. This will display all the commands that begins with that string.

4.2.1.5 Input verification

4.2.1.5.1 Returned Information: success

All commands entered through keyboards undergo syntax check by the Shell. Nothing will be

returned if the user entered a correct command under corresponding modes and the execution is successful.

4.2.1.5.2 Returned Information: error

Output error message	Explanation
Unrecognized command or illegal parameter!	The entered command does not exist, or there is error in parameter scope, type or format.
Ambiguous command	At least two interpretation are possible based on the current input.
Invalid command or parameter	The command is recognized, but no valid parameter record is found.
This command does not exist in current mode	The command is recognized, but this command can not be used under current mode.
Please configure precursor command "*" at first!	The command is recognized, but the prerequisite command has not been configured.
Syntax error: missing "" before the end of command line!	Quotation marks are not used in pairs.

4.2.1.6 Fuzzy match support

ES4704BD Shell support fuzzy match in searching for commands and keywords. Shell will recognize commands or keywords correctly if the entered string causes no conflict.

For example:

1. For Admin configuration command “show interface ethernet 1/1”, simply typing in “sh in e 1/1” will work.
2. However, for Admin configuration command “show running-config”, the system will, if only “show r” is entered, report a “> Ambiguous command!” error. Shell is unable to tell whether it is “show rom” or “show running-config”. Therefore, Shell will only recognize the command if the minimum of “sh ru” is entered.

4.3 Web Management

4.3.1 Main Page

ES4704BD routing switch provides HTTP web management function and users can configure and monitor the status of the switch through the web interface.

To manage the switch through web browser use the following steps:

Configure valid IP address, mask and confirm gateway for the switch. Please reference to 5.3

1. Configure web user management and its password
2. Connect to the switch using the web browser. Enter the username and password to proceed to web management.

4.3.2 Module Front Panel

When entering username, password and passing authentication, you will see the following web management main page. On the left of the management page is the main management menu and on the right of the page system information and command parameter are displayed. Click the main menu link to browse other management links and to display configuration and statistic information.

Chapter 5 Basic Switch Configuration

5.1 Basic Switch Configuration Commands

This section covers the basic configuration for the switch, including all the commands for entering and exiting the Admin Mode and Interface Mode, setting and displaying switch clock and displaying system version information.

5.1.1 clock set

Command: clock set <*HH:MM:SS*> <*YYYY.MM.DD*>

Function: Sets system date and time.

Parameters: <***HH:MM:SS*** > is the current time, and the valid scope for ***HH*** is 0 to 23, ***MM*** and ***SS*** is 0 to 59; <***YYYY.MM.DD*** > is the current year, month and date. The valid scope for ***YYYY*** is 1970~2100, ***MM*** *is* between 1 to 12， and ***DD*** is between 1 and 31.

Command mode: Admin Mode

Default: upon first time start-up, defaulted is 2001.1.1 0:0:0.

Usage guide: The switch can not continue keeping time with power off, hence the current date and time must be first set at environments where exact time is required.

Example: Setting the switch current date and time to 2002.8.1 23:0:0:

Switch#clock set 23:0:0 2002.8.1

Related command: show clock

5.1.2 config

Command: config [terminal]

Function: Enters Global Mode from Admin Mode.

Parameters: [terminal] indicates terminal configuration.

Command mode: Admin Mode

Example:

Switch#config

5.1.3 enable

Command: enable

Function: Enter Admin Mode from User Mode.

Command mode: User Mode

Usage Guide: To prevent unauthorized access of non-admin users, user authentication is required (i.e., Admin user password is required) when entering Admin Mode from User Mode. If the correct Admin user password is entered, Admin Mode access is granted. If 3 consecutive entries of Admin

user password are all wrong, it remains in the User Mode. Set the Admin user password under Global Mode with the "**enable password**" command.

Example:

Switch>enable

password: ***** (admin)

Switch#

Related command: enable password

5.1.4 enable password

Command: enable password

Function: Modify the password to enter Admin Mode from the User Mode, press Enter after type in this command displays **<*Current password*>** and **<*New password*>** parameter for the users to configure.

Parameters: **<*Current password*>** is the original password, up to 16 characters are allowed; **<*New password*>** is the new password, up to 16 characters are allowed; **<*Confirm new password*>** is to confirm the new password and should be the same as **<*New password*>**, otherwise, the password will need to be set again.

Command mode: Global Mode

Default: upon first time start-up, the Admin user password is empty. If this is the first configuration, simply press Enter on prompting for current password.

Usage Guide: Configure Admin user password to prevent unauthorized access from non-admin user. It is recommended to set the Admin user password at the initial switch configuration. Also, it is recommended to exit Admin Mode with "**exit**" command when the administrator need to leave the terminal for a long time.

Example: Setting the Admin user password to "admin".

Switch(Config)#enable password

Current password: (First time configuration, no password set, just press Enter)

New password:***** (Type in admin to set the new password to "admin")

Confirm New password:***** (Type admin again to confirm the new password)

Switch(Config)#

Related command: enable

5.1.5 exec timeout

Command: exec timeout <*minutes* >

Function: Sets timeout value for exiting Admin Mode

Parameters: **< *minute* >** is the time in minutes, the valid range is 0 to 300.

Command mode: Global Mode

Default: The default value is 5 minutes.

Usage Guide: To ensure security for the switch and prevent malicious operation of unauthorized users, timeout count will start after the last configuration by the Admin user. The system will automatically exit the Admin Mode upon the preset timeout threshold. If the user needs to enter Admin Mode, the Admin user password needs to be entered again. A 0 exec timeout value indicates the system will never exit Admin Mode automatically.

Example: Setting timeout value for the switch to exit Admin Mode to 6 minutes.

Switch(Config)#exec timeout 6

5.1.6 exit

Command: exit

Function: Exits the current mode to the previous mode. Under Global Mode, this command will return the user to Admin Mode, and in Admin Mode to User Mode, etc.

Command mode: All configuration modes.

Example:

Switch#exit

Switch>

5.1.7 help

Command: help

Function: Outputs brief descriptions of the command interpreter help system.

Command mode: All configuration modes.

Usage Guide: A instant online help provided by the switch. Help command displays information about the whole help system, including complete help and partial help. The user can type in ? any time to get online help.

Example:

Switch>help

enable	-- Enable Privileged mode
exit	-- Exit telnet session
help	-- help
show	-- Show running system information

5.1.8 ip host

Command: ip host <*hostname*> <*ip_addr*>

no ip host <*hostname*>

Function: Sets the mapping relationship between the host and IP address; the “no ip host” parameter of this command deletes the mapping.

Parameters: <***hostname***> is the host name, up to 15 characters are allowed; <***ip_addr***> is the corresponding IP address for the host name and takes a decimal format.

Command mode: Global Mode

Usage Guide: Sets the association between host and IP address, which can be used in commands like **"ping <host>**".

Example: Setting the IP address of a host with the hostname of "ES4704BD" to 200.121.1.1.

Switch(Config)#ip host ES4704BD 200.121.1.1

Related commands: telnet, ping, traceroute

5.1.9 hostname

Command: hostname <*hostname*>

Function: Sets the prompt in the switch command line interface.

Parameter **<*hostname*>** is the string for the prompt, up to 30 characters are allowed.

Command mode: Global Mode

Default: The default prompt is ES4704BD.

Usage Guide: With this command, the user can set the command line prompt of the switch according to their own requirements.

Example: Setting the prompt to "Test".

Switch(Config)#hostname Test

Test(Config)#

5.1.10 reload

Command: reload

Function: Warm resets the switch.

Command mode: Admin Mode

Usage Guide: The user can use this command to restart the switch without power off .

5.1.11 set default

Command: set default

Function: Resets the switch to factory settings.

Command mode: Admin Mode

Usage Guide: Resets the switch to factory settings. That is to say, all configurations made by the user to the switch will disappear. When the switch is restarted, the prompt will be the same as when the switch was powered on for the first time.

Note: After use of this command, "**write**" command must be executed in order to save the operation. The switch will reset to factory settings after restart.

Example:

Switch#set default

Are you sure? [Y/N] = y

Switch#write

Switch#reload

5.1.12 setup

Command: setup

Function: Enters the Setup Mode of the switch.

Command mode: Admin Mode

Usage Guide: ES4704BD provides a Setup Mode, in which the user can configure IP addresses, etc.

5.1.13 language

Command: language {chinese|english}

Function: Sets the language for displaying the help information.

Parameters: chinese for Chinese display; english for English display.

Command mode: Admin Mode

Default: The default setting is English..

Usage Guide: ES4704BD provides help information in two languages, the user can select the language according to their preference. After the system restart, the help information display will revert to English.

5.1.14 write

Command: write

Function: Saves the currently configured parameters to the Flash memory.

Command mode: Admin Mode

Usage Guide: After a set of configurations with desired functions, the setting should be saved to the Flash memory, so that the system can revert to the saved configuration automatically in the case of accidental power down or power failure. This is the equivalent to the **copy running-config startup-config** command.

Related commands: copy running-config startup-config

5.2 Maintenance and Debug Commands

When users configure the switch, they will need to verify whether the configurations are correct and the switch is operating as expected, and in the case of network failure, the users will also need to diagnose the problem. ES4704BD provides various debugging methods including ping, Telnet, show, debug, etc. to help the users to check system configuration, operating status and locate problem causes.

5.2.1 ping

Command: ping [<*ip-addr*>]

Function: The switch sends an ICMP packet to remote devices to verify the connectivity between

the switch and remote devices.

Parameters: <*ip-addr*> is the target host IP address for ping, in decimal format.

Default: Sends 5 ICMP packets of 56 bytes each, timeout is 2 seconds.

Command mode: Admin Mode

Usage Guide: When the user types in the **ping** command and press Enter, the system will provide an interactive mode for configuration, and the user can choose all the parameters for **ping**.

Example:

Example 1: Default parameter for **ping.**

Switch#ping 10.1.128.160

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.

...!!

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

As shown in the above example, the switch pings a device with an IP address of 10.1.128.160, three ICMP request packets were sent without receiving corresponding reply packets (i.e., ping failed), the last two packets were successfully replied, the successful rate was 40%. The switch represent ping failure with a ".", for unreachable targets; and represents ping success with "!" , for reachable targets.

Switch#ping

protocol [IP]：

Target IP address：10.1.128.160

Repeat count [5]：100

Datagram size in byte [56]：1000

Timeout in milli-seconds [2000]：500

Extended commands [n]：n

Displayed information	Explanation
Protocol [IP]	Selects the **ping** for IP protocol
Target IP address	Target IP address
Repeat count [5]	Packet number, the default is 5
Datagram size in byte [56]	ICMP packet size the default is 56 bytes
Timeout in milli-seconds [2000]	Timeout (in milliseconds,) the default is 2 seconds
Extended commands [n]	Whether to change the other options or not

5.2.2 Telnet

5.2.2.1 Introduction to Telnet

Telnet is a simple remote terminal protocol for remote login. Using Telnet, the user can login to a remote host with its IP address of hostname from his own workstation. Telnet can send the user's keystrokes to a remote host and send the remote host's output to the user's screen through a TCP connection. This is a transparent service. To the user, the keyboard and monitor seem to be connected to the remote host directly.

Telnet employs the Client-Server mode, the local system is the Telnet client and the remote host is the Telnet server. ES4704BD can be either the Telnet Server or the Telnet client.

When ES4704BD is used as the Telnet server, the user can use the Telnet client program included in Windows or the other operating systems to login to ES4704BD, as described earlier in the In-band management section. As a Telnet server, ES4704BD allows up to 5 telnet client TCP connections.

As Telnet client, ES4704BD uses **telnet** command under the Admin Mode to allow the user to log in to the other remote hosts. ES4704BD can only establish TCP connections to one remote host at a time. If a connection to another remote host is desired, the current connection must be dropped.

5.2.2.2 Telnet Task Sequence

1. Configure the Telnet Server
2. Telnet to a remote host from the switch.

1. Configuring Telnet Server

Command	Explanation
Global Mode	
telnet-server enable **no telnet-server enable**	Enables the Telnet server function in the switch: the "**no telnet-server enable"** command disables the Telnet function.
telnet-user <*user-name*> password {0|7} <*password*> **no telnet-user <*user-name*>**	Configures the username and password to Telnet the switch: the **"no telnet-user <user-name>"** command deletes the authorized Telnet user.
telnet-server securityip <*ip-addr*> **no telnet-server securityip <*ip-addr*>**	Configures the secure IP address to login to the switch through Telnet: the "**no telnet-server securityip <*ip-addr*>"** command deletes the authorized Telnet secure address.
Admin Mode	
monitor	Displays debug information for Telnet

no monitor	client login to the switch; the "**no monitor"** command disables the debug information.

2. Telnet to a remote host from the switch

Command	Explanation
Admin Mode	
telnet [<*ip-addr*>] [<*port*>]	Logs in to a remote host with the Telnet client included in the switch.

5.2.2.3 Telnet Commands

5.2.2.3.1 monitor

Command: monitor

no monitor

Function: Enables debugging information for Telnet clients logged in to the switch, the Console end debug display will be disabled at the same time; the "no monitor" command disables the debug information and re-enables the Console end debug display.

Command mode: Admin Mode

Usage Guide: When a Telnet client accessing the switch enables Debug information, the information is not shown in the Telnet interface, instead, it is displayed in the terminal connecting to the Console port. This command specifies the debugging information to be displayed in the Telnet terminal screen instead of the Console or other Telnet terminal screens.

Example: Enabling the display the debug information in Telnet client.

Switch#monitor

Related command: telnet-user

5.2.2.3.2 telnet

Command: telnet [<*ip-addr*>] [<*port*>]

Function: Logs in to a remote host with an IP address of **<*ip-addr*>** through Telnet.

Parameters: <*ip-addr*> is the remote host IP address in decimal format. **<*port*>** is the port number, valid values are from 0 – 65535.

Command mode: Admin Mode

Usage Guide: This command is used when the switch is used as a client, the user logs in to remote hosts for configuration with this command. ES4704BD can only establish TCP connection to one remote host as a Telnet client. If a connection to another remote host is desired, the current TCP connection must be dropped. To disconnect with a remote host, the shortcut key combination

"CTRL+|" can be used.

Input **Telnet** keyword without any parameters to enter the Telnet configuration mode.

Example: Telnet to a remote router with the IP address 20.1.1.1 from the switch.

Switch#telnet 20.1.1.1 23

Connecting Host 20.1.1.123 Port 23...

Service port is 23

Connected to 20.1.1.123login:123

password:***

router>

5.2.2.3.3 telnet-server enable

Command: telnet-server enable

no telnet-server enable

Function: Enables the Telnet server function in the switch: the "**no telnet-server enable"** command disables the Telnet function in the switch.

Default: Telnet server function is enabled by default.

Command mode: Global Mode

Usage Guide: This command is available in Console only. The administrator can use this command to enable or disable the Telnet client from logging into the switch.

Example: Disabling the Telnet server function in the switch.

Switch(Config)#no telnet-server enable

5.2.2.3.4 telnet-server securityip

Command: telnet-server securityip <*ip-addr*>

no telnet-server securityip <*ip-addr*>

Function: Configures the secure IP address of Telnet clients allowed to log in to the switch; the "**no telnet-server securityip <*ip-addr*>"** command deletes the authorized Telnet secure address.

Parameters: <*ip-addr*> is the secure IP address allowed to access the switch, in decimal format.

Default: no secure IP addresses are set by default.

Command mode: Global Mode

Usage Guide: When no secure IP addresses are configured, the IP addresses of Telnet clients connecting to the switch will not be limited; if secure IP addresses are configured, only hosts with a secure IP address is allowed to connect to the switch through Telnet for configuration. The switch allows multiple secure IP addresses.

Example: Setting 192.168.1.21 as a secure IP address.

Switch(Config)#telnet-server securityip 192.168.1.21

5.2.2.3.5 telnet-user

Command: telnet-user <*username*> password {0|7} <*password*>

no telnet-user <*username*>

Function: Sets the username and password for the Telnet client; the **"no telnet-user <user-name>"** command deletes the specified Telnet user.

Parameters: **<*username*>** is the Telnet client's username, up to 16 characters are allowed; **<*password*>** is the login password, up to 8 characters are allowed; 0|7 indicate non-masked password display and masked password display.

Command mode: Global Mode

Default: No Telnet client username and password is set by default.

Usage Guide: This command is used when the switch is used as a server, this command is used to set authorized Telnet clients. If the Telnet function authorization has not been configured, nobody can connect via Telnet for configuration. As a Telnet server, ES4704BD allows up to 5 telnet client TCP connections.

Example: Setting a Telnet client user, with username of "Antony" and password of "switch".

Switch(Config)#telnet-user Antony password 0 switch

5.2.3 traceroute

Command: traceroute {<*ip-addr*> | host <*hostname*> }[hops <*hops*>] [timeout <*timeout*>]

Function: This command tests the gateway passed while packet is in route from the source device to the target device. This can be used to test connectivity and locate a failed sector.

Parameters: **<*ip-addr*>** is the target host IP address in decimal format. **<*hostname*>** is the hostname for the remote host. **<*hops*>** is the maximum gateway number allowed by the Traceroute command. **<*timeout*>** is the timeout value for test packets in milliseconds, between 100 – 10000.

Default: The default maximum gateway number is 16, timeout is 2000 ms.

Command mode: Admin Mode

Usage Guide: Traceroute is usually used to locate the problem for unreachable network nodes.

Related command: ip host

5.2.4 show

show command is used to display information about the system, such as port and protocol operations. This part introduces the **show** command that displays system information, other **show** commands will be discussed in other chapters.

5.2.4.1 show clock

Command: show clock

Function: Displays the system clock.

Command mode: Admin Mode

Usage Guide: The user can use this command to check the system date and time so that the system clock can be adjusted if an inaccuracy occurs.

Example:

Switch#show clock

Current time is TUE AUG 22 11：00：01 2002

Related command: clock set

5.2.4.2 show debugging

Command: show debugging

Function: Displays the debugging switch status.

Usage Guide: If a user needs to check what debugging switches have been enabled, **show debugging** command can be executed.

Command mode: Admin Mode

Example: Checking for currently enabled debugging switch.

Switch#show debugging

STP:

Stp input packet debugging is on

Stp output packet debugging is on

Stp basic debugging is on

Switch#

Related command: debug

5.2.4.3 show flash

Command: show flash

Function: Displays the files and their sizes in the Flash memory.

Command mode: Admin Mode

Example: Checking for files and their sizes in the Flash memory.

Switch#show flash

boot.rom	329,828 1900-01-01 00:00:00 --SH
boot.conf	94 1900-01-01 00:00:00 --SH
nos.img	2,449,496 1980-01-01 00:01:06 ----
startup-config	2,064 1980-01-01 00:30:12 ----

5.2.4.4 show history

Command: show history

Function: Displays the recent user’s command history

Command mode: Admin Mode

Usage Guide: The system holds up to 10 commands entered by the user, the user can press the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example:

Switch#show history

enable

config

interface ethernet 1/3

enable

show flash

show ftp

5.2.4.5 show memory

Command: show memory

Function: Displays the contents in the memory.

Command mode: Admin Mode

Usage Guide: This command is used for switch debugging purposes. The command will interactively prompt the user to enter start address of the desired information in the memory and output word number. The displayed information consists of three parts: address, Hex view of the information, character view

Example:

Switch#show memory

start address : 0x2100

number of words[64]:

002100: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002110: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002120: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002130: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002140: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002150: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002160: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

002170: 0000 0000 0000 0000 0000 0000 0000 0000 *.....*

5.2.4.6 show running-config

Command: show running-config

Function: Displays the current active configuration parameters for the switch.

Default: If the active configuration parameters are the same as the default operating parameters,

nothing will be displayed.

Command mode: Admin Mode

Usage Guide: When the user finishes a set of configurations and needs to verify the configurations, show running-config command can be used to display the current active parameters.

Example:

Switch#show running-config

5.2.4.7 show startup-config

Command: show startup-config

Function: Displays the switch parameter configurations written in the Flash memory at the current operation, those are usually also the configuration files used for the next power-up.

Default: If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations while **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash memory, the displays of **show running-config** and **show startup-config** will be the same.

5.2.4.8 show switchport interface

Command: show switchport interface [ethernet <interface-list>]

Function: Displays VLAN interface mode, LAN number, and Trunk port information for the switch.

Parameters: <*interface-list*> is the port number or a port list, which can be for any port information existing in the switch.

Command mode: Admin Mode

Example: Displays the VLAN information for interface ethernet 1/1.

Switch#show switchport interface ethernet 1/1
Ethernet1/1
Type :Universal
Mac addr num :-1
Mode :Access
Port VID :1
Trunk allowed Vlan :ALL

Displayed information	Description
Ethernet1/1	Corresponding Ethernet interface number
Type	Current Interface Type
Mac addr num	MAC address number can be learned by the current

	interface
Mode :Access	VLAN mode of the current Interface
Port VID :1	VLAN number belong to the current Interface
Trunk allowed Vlan :ALL	VLAN allowed to be crossed by Trunk.

5.2.4.9 show tcp

Command: show tcp

Function: Displays the current TCP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show tcp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	23	0.0.0.0	0	LISTEN
0.0.0.0	80	0.0.0.0	0	LISTEN

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local pot number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

5.2.4.10 show udp

Command: show udp

Function: Displays the current UDP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show udp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	161	0.0.0.0	0	CLOSED
0.0.0.0	123	0.0.0.0	0	CLOSED
0.0.0.0	1985	0.0.0.0	0	CLOSED

Displayed information	Description
LocalAddress	Local address of the UDP connection
LocalPort	Local pot number of the UDP connection
ForeignAddress	Remote address of the UDP connection
ForeignPort	Remote port number of the UDP connection
State	Current status of the UDP connection

5.2.4.11 show telnet login

Command: show telnet login

Function: Displays the current Telnet client information that is connected to the switch.

Usage Guide: This command can be used to check the information of currently logged in remote users.

Example:
Switch#show telnet login

Authenticate login by local.

Login user:

aa

Switch#

5.2.4.12 show telnet user

Command: show telnet user

Function: Displays authorized Telnet client's information

Usage Guide: This command can be used to check for all current authorized Telnet clients.

Example:

Switch#show telnet user

Antony

Switch#

Related command: telnet-user password

5.2.4.13 show version

Command: show version

Function: Displays the switch version.

Command mode: Admin Mode

Usage Guide: Use this command to view the version information for the switch, including hardware version and software version.

Example:

Switch#show vers

ES4704BD Device, Apr 14 2005 11:19:29

HardWare version is , SoftWare version is ES4704BD_1.0.6.0, BootRom version is ES4704BD_1.4.1

Copyright (C) 2001-2004 by Edge-Core Networks Limited.

All rights reserved.

Switch#

5.2.5 debug

All the protocols ES4704BD supports have their corresponding debugging commands. The users can use the information from the debugging command for troubleshooting. Debugging commands for their corresponding protocols will be introduced in the later chapters.

5.3 Configuring Switch IP Addresses

All Ethernet ports of ES4704BD perform layer 2 forwarding. The VLAN interface represents a Layer 3 interface function, which can be assigned an IP address, this is also the IP address of the switch. All VLAN interface related configuration commands can be configured under VLAN Mode. ES4704BD provides three IP address configuration methods:

- ☞ Manual
- ☞ BootP
- ☞ DHCP

Manual configuration of IP address is assign an IP address manually for the switch.

In BootP/DHCP mode, the switch operates as a BootP/DHCP client. It sends broadcast packets of BootPRequest to the BootP/DHCP servers. The BootP/DHCP servers then assign the address upon receiving the request. In addition, ES4704BD can act as a DHCP server, and dynamically assign network parameters such as IP addresses, gateway addresses and DNS server addresses to DHCP clients. DHCP Server configurations are detailed in later chapters.

5.3.1 Configuring Switch IP Addresses Task Sequence

1. Manual configuration
2. BootP configuration
3. DHCP configuration

1. Manual configuration

Command	Explanation
ip address <*ip_address*> <*mask*> [secondary] **no ip address <*ip_address*> <*mask*> [secondary]**	Configures the VLAN interface IP address; the "**no ip address <*ip_address*> <*mask*> [secondary]"** command deletes VLAN interface IP address.

2. BootP configuration

Command	Explanation
ip bootp-client enable	Enables the switch to be a BootP client and

no ip bootp-client enable	obtain an IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP client function.

3.DHCP

Command	Explanation
ip dhcp-client enable **no ip dhcp-client enable**	Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp-client enable**" command disables the DHCP client function.

5.3.2 Commands for Configuring Switch IP Addresses

5.3.2.1 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Sets the IP address and mask for the specified VLAN interface; the "**no ip address <*ip address*> <*mask*> [secondary]"** command deletes the specified IP address setting.

Parameters: <*ip-address*> is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format; **[secondary]** indicates the IP configured is a secondary IP address

Default: No IP address is configured upon switch shipment.

Command mode: VLAN Interface Mode

Usage Guide: A VLAN interface must be created first before the user can assign an IP address to the switch.

Example: Set 10.1.128.1/24 as the IP address of VLAN1 interface.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip address 10.1.128.1 255.255.255.0

Switch(Config-If-Vlan1)#exit

Switch(Config)#

Related command: ip bootp-client enable, ip dhcp-client enable

5.3.2.2 ip bootp-client enable

Command: ip bootp-client enable

no ip bootp-client enable

Function: Enable the switch to be a BootP client and obtain IP address and gateway address through BootP negotiation; the "**no ip bootp-client enable**" command disables the BootP client function and releases the IP address obtained in BootP .

Default: BootP client function is disabled by default.

Command mode: VLAN Interface Mode

Usage Guide: Obtaining IP address through BootP, Manual configuration and DHCP are mutually exclusive, enabling any 2 methods for obtaining IP address is not allowed. Note: To obtain IP address via DHCP, a DHCP server or a BootP server is required in the network.

Example: Get IP address through BootP.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip bootp-client enable

Switch (Config-If-Vlan1)#exit

Switch (Config)#

Related command: ip address, ip dhcp-client enable

5.3.2.3 ip dhcp-client enable

Command: ip dhcp-client enable

no ip dhcp-client enable

Function: Enables the switch to be a DHCP client and obtain IP address and gateway address through DHCP negotiation; the "**no ip dhcp -client enable**" command disables the DHCP client function and releases the IP address obtained in DHCP. Note: To obtain IP address via DHCP, a DHCP server is required in the network.

Default: the DHCP client function is disabled by default.

Command mode: VLAN Interface Mode

Usage Guide: Obtaining IP address by DHCP, Manual configuration and BootP are mutually exclusive, enabling any 2 methods for obtaining an IP address is not allowed.

Example: Getting an IP address through DHCP.

Switch (Config)#interface vlan 1

Switch (Config-If-Vlan1)#ip dhcp-client enable

Switch (Config-If-Vlan1)#exit

Switch (Config)#

Related command: ip address, ip bootp-client enable

5.4 Configuring SNMP

5.4.1 Introduction to SNMP

SNMP (Simple Network Management Protocol) is a standard inter-network management protocol widely used in computer network management. SNMP is an evolving protocol. SNMP v1[RFC1157] is the first version of SNMP. SNMP v1 has been adapted by vast numbers of manufacturers for its simplicity and easy implementation. With enhancements into both functions

and security, SNMP developed to its second version, SNMP v2. As it is still based on SNMP v1, we will focus on SNMP v1. In this manual, if not otherwise specified, SNMP refers to v1.

SNMP protocol provide a relatively direct way of exchanging management information between two points in the network. SNMP employs a polling mechanism of message query transmitted through UDP (a connectionless transport layer protocol), and is therefore well supported by the existing computer networks.

SNMP protocol works in NMS(Network Management Station)-Agent mode, thus consists of two parts: NMS and Agent. NMS is the workstation to run a SNMP enabled network administration client program and is the core in SNMP network administration. Agent is the server software running on the device to be managed and handles the managed objects directly. NMS handles all the managed objects through Agents.

The NMS and Agent of SNMP communicate in Client/Server mode with standard messages, the NMS sends requests and the Agent responds. There are 5 SNMP message types:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

NMS sends queries and management variable setting requests to the Agent with Get-Request, Get-Next-Request and Set-Request messages. Then, upon receiving the requests, the Agent replies with a Get-Response message. In some special situations, when network device ports Up/Down status or network topology changes, Agents will send Trap messages to NMS to inform the NMS of exceptions. NMS can also be set to alert some exceptions by enabling RMON. When preset alert events are triggered, Agents will send Trap messages or log the event according to these settings.

The security mechanism of SNMP protocol is not so comprehensive, the main security method is the use of community strings. A Community string is a kind of access password set in the Agent. Read/write access permission is set for each community string in the Agent. NMS must include the community string in the packets sent to Agent, otherwise it won't be granted corresponding read/write permission to access the Agent.

5.4.2 Introduction to MIB

The network administrative information that NMS can access is well defined and organized in a Management Information Base (MIB). MIB is a accurate definition to the information that can be accessed by network administrative protocols. It takes a layered and structured form, so defined management information can be obtained from monitored network devices. ISO ASN.1 defines a tree structure for MIB, each MIB organizes all the available information with this tree structure, each node contains an OID (Object Identifier) and a brief text description about the node. OID is a set of integers divided by periods, it identifies the node and can be used to locate the node in a MIB

tree structure, as show in the figure below:

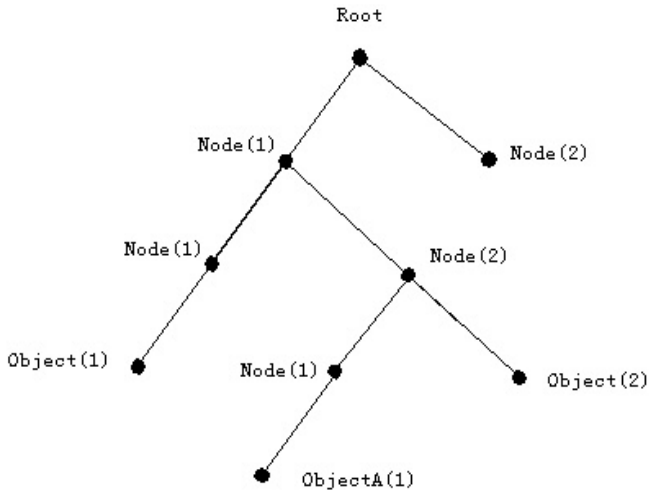


Fig 5-1 ASN.1 tree instance

In this figure, the OID of object A is 1.2.1.1. NMS can find this object without ambiguity through the object's unique OID to get the standard variable contained in the object. MIB will define a set of standard variables for monitored network devices according to this structure.

If the variable information inside Agent MIB needs to be browsed, MIB browsing software needs to be run in NMS, such as the MIB browser included in ECview. MIBs in the Agent usually consists of public MIB and private MIB. The public MIB contains public network management information that can be accessed by all NMS; private MIB contains property information specific to all the devices. Device manufacturer support is required for NMS to browse and manage the private MIB.

MIB-I [RFC1156] is the first implementation of SNMP public MIB, and was replaced by MIB-II [RFC1213]. MIB-II expanded MIB-I but kept its OID of MIB tree. MIB-II contains many sub-trees, referred to as groups. Objects in these groups cover all the functional domains in network management. NMS obtains corresponding network management information by visiting the MIB of the SNMP Agent.

ES4704BD can operate as a SNMP Agent, and supports both SNMP v1 and v2c, basic MIB-II, RMON public MIB and other related public MIBs such as BRIDGE MIB.

5.4.3 Introduction to RMON

RMON is the most important expansion to the standard SNMP basic architecture. RMON is a set of MIB definitions used to define standard network monitoring functions and interfaces, and enabling communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

RMON's MIB consists of 10 groups, ES4704BD support the most frequently used groups: 1, 2, 3, 9

Statistics: Maintains basic utilization and error statistics for each subnet monitored by the Agent.

History: Records periodical statistic samples available from Statistics.

Alarm: Allows users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.

Event: A list of all events generated by RMON Agent.

Alert depends on the implementation of Event. Statistics and History display some current or history subnet statistics. Alert and Event provide a method to monitor any integer data change in the network, and provide some alerts upon exceptions (sending Trap or record in logs).

5.4.4 Configuring SNMP

5.4.4.1 SNMP Configuration Task Sequence

1. Enable or disable SNMP Agent server function
2. Configure SNMP community string
3. Configure secure address of SNMP management base
4. Configuring TRAP
5. Enable/Disable RMON

1. Enable or disable SNMP Agent server function

Command	Explanation
snmp-server enable **no snmp-server enable**	Enables the SNMP agent server function in the switch: the "**no snmp-server enable"** command disables the SNMP agent server function**.**

2. Configure SNMP community string

Command	Explanation
snmp-server community {ro|rw} <***string***> **no snmp-server community** <***string***>	Configures the community string for the switch: the "**no snmp-server community** <***string***>" command deletes the configured community string.

3. Configure secure address for SNMP management

Command	Explanation
snmp-server securityip <***ip-address***>	Configures the secure IP address for NMS

no snmp-server securityip <*ip-address*>	allowed to access the switch: "**no snmp-server securityip <*ip-address*>**" command deletes the configured secure address.

4. Configuring TRAP

Command	Explanation
snmp-server enable traps **no snmp-server enable traps**	Sets the switch to enable to send Trap messages; the "**no snmp-server enable traps**" command disables Trap messages.
snmp-server host <*host-addr*> <*community-string*> **no snmp-server host <*host-addr*>**	Sets the IP address and Trap community string of the NMS to receive SNMP trap messages; the "**no snmp-server host <*host-addr*>**" command deletes the IP address of the NMS to receive SNMP Trap messages.

5. Enable/Disable RMON

Command	Explanation
rmon enable **no rmon enable**	Enables/Disables RMON

5.4.4.2 SNMP Configuration Commands

5.4.4.2.1 rmon

Command: rmon enable

no rmon enable

Function: Enables the RMON function in the switch: the "no rmon enable**" command disables the RMON function.**

Command mode: Global Mode

Default: RMON is enabled by default.

Example:

Enabling RMON.

Switch(Config)#rmon enable

Disabling RMON.

Switch(Config)#no rmon enable

5.4.4.2.2 snmp-server community

Command: snmp-server community {ro|rw} <*string*>

no snmp-server community <*string*>

Function: Configures the community string for the switch: the "**no snmp-server community <*string*>**" command deletes the configured community string.

Command mode: Global Mode

Parameters: **<*string*>** is the community string set; **ro|rw** is the specified access mode to MIB, **ro** for read-only and **rw** for read-write.

Usage Guide: Up to 4 community strings are supported by the switch.

Example: Adding a community string named "private" with read-write permission.

Switch(Config)#snmp-server community rw private

Add a community string named "public" with read-only permission.

Switch(Config)#snmp-server community ro public

Modify the read-write community string named "private" to read-only.

Switch(Config)#snmp-server community ro private

Delete community string "private".

Switch(Config)#no snmp-server community private

5.4.4.2.3 snmp-server enable

Command: snmp-server enable

no snmp-server enable

Function: Enables the SNMP agent server function in the switch: the "**no snmp-server enable"** command disables the SNMP agent server function**.**

Command mode: Global Mode

Default: SNMP agent server function is disabled by default.

Usage Guide: To enable configuration and management via network administrative software, this command must be executed to enable the SNMP agent server function for the switch.

Example: Enabling SNMP Agent server function for the switch.

Switch(Config)#snmp-server enable

5.4.4.2.4 snmp-server enable traps

Command: snmp-server enable traps

no snmp-server enable traps

Function: Sets to enable the switch to send Trap message; the "**no snmp-server enable traps**" command disables Trap messages.

Command mode: Global Mode

Default: Trap message is disabled by default. .

Usage Guide: When Trap message is enabled, if Down/Up in device ports or of system occurs, the device will send Trap messages to NMS that receives Trap messages.

Example:

Enable sending of Trap messages.

Switch(Config)#snmp-server enable traps

Disable sending of Trap messages

Switch(Config)#no snmp-server enable trap

5.4.4.2.5 snmp-server host

Command: snmp-server host <*host-addr*> <*community-string*>

no snmp-server host <*host-addr*>

Function: Sets the IP address and Trap community string of the NMS to receive SNMP trap message; the "**no snmp-server host <*host-addr*>**" command deletes the IP address of the NMS to receive SNMP Trap message.

Command mode: Global Mode

Parameters: <*host-addr*> is the IP address of NMS to receive Trap messages; **<*community-string*>** is the community string used in sending Trap message.

Usage Guide: This command sets community string used to send Trap message, the string is also the default RMON Event community string. If RMON Event has no community string set, the community string set with this command will be used to send RMON Trap; if RMON Event has a community string set, the RMON community string will be used to send RMON Trap

Example:

Set an IP address to receive Trap.

Switch(Config)#snmp-server host 1.1.1.5 dcstrap

Delete an IP address that receives Trap.

Switch(Config)#no snmp-server host 1.1.1.5

5.4.4.2.6 snmp-server securityip

Command: snmp-server securityip <*ip-address*>

no snmp-server securityip <*ip-address*>

Function: Configures the secure IP address for NMS allowed to access the switch: the "**no snmp-server securityip <*ip-address*>**" command deletes configured secure address.

Command mode: Global Mode

Parameters: <*ip-address*> is the NMS secure IP address, in decimal format.

Usage Guide: The SNMP packet sent by NMS will only be processed by the switch if the NMS IP address matches the secure IP address set with this command.

Example:

Set the secure IP address for NMS.

Switch(Config)#snmp-server securityip 1.1.1.5

Delete a secure IP address.

Switch(Config)#no snmp-server securityip 1.1.1.5

5.4.5 Typical SNMP Configuration Examples

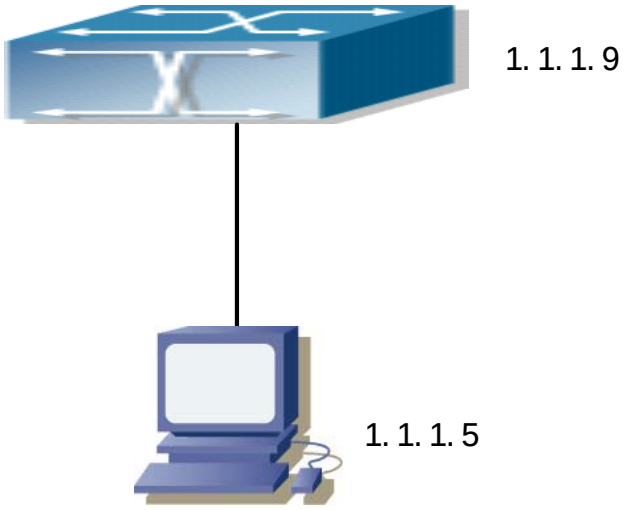


Fig 5-2 SNMP Configuration Example

The IP address of NMS is 1.1.1.5; the Switch (Agent) IP address is 1.1.1.9.

Scenario 1: The NMS network administrative software uses SNMP protocol to obtain data from the switch.

The configuration of the switch is listed below:

Switch(Config)#snmp-server enable

Switch(Config)#snmp-server community rw private

Switch(Config)#snmp-server community ro public

Switch(Config)#snmp-server securityip 1.1.1.5

Thus, the NMS can use “private” as the community string to access the switch with read-write permission, or use “public” as the community string to access the switch with read-only permission.

Scenario 2: NMS will receive Trap messages from the switch (note: NMS may have community string verification for the Trap messages, in this scenario, the NMS uses a Trap verification community string of “dcstrap”).

The configuration of the switch is listed below:

Switch(Config)#snmp-server host 1.1.1.5 dcstrap

Switch(Config)#snmp-server enable traps

5.4.6 SNMP Troubleshooting Help

5.4.6.1 Monitor and Debug Commands

5.4.6.1.1 show snmp

Command: show snmp

Function: Displays all SNMP counter information.

Command mode: Admin Mode

Example:

Switch#show snmp

0 SNMP packets input

0 Bad SNMP version errors

0 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

0 SNMP packets output

0 Too big errors (Max packet size 1500)

0 No such name errors

0 Bad values errors

0 General errors

0 Get-response PDUs

0 SNMP trap PDUs

Displayed information	Explanation
snmp packets input	Total number of SNMP packet inputs
bad snmp version errors	Number of version information error packets
unknown community name	Number of community name error packets
illegal operation for community name supplied	Number of permission for community name error packets
encoding errors	Number of encoding error packets
number of requested variables	Number of variables requested by NMS
number of altered variables	Number of variables set by NMS
get-request PDUs	Number of packets received by “get” requests
get-next PDUs	Number of packets received by “getnext”

	requests
set-request PDUs	Number of packets received by “set” requests
snmp packets output	Total number of SNMP packet outputs
too big errors	Number of “Too_ big” error SNMP packets
maximum packet size	Maximum length of SNMP packets
no such name errors	Number of packets requesting for non-existent MIB objects
bad values errors	Number of “Bad_values” error SNMP packets
general errors	Number of “General_errors” error SNMP packets
response PDUs	Number of response packets sent
trap PDUs	Number of Trap packets sent

5.4.6.1.2 show snmp status

Command: show snmp status

Function: Displays SNMP configuration information.

Command mode: Admin Mode

Example:

Switch#show snmp status

System Name:

System Contact:

System Location:

Trap enable

RMON enable

Community Information:

Trap manager Information:

Security IP Information:

****

Displayed information	Description
System Name	System name
System Contact	System Contact Method
System Location	System location
Trap enable	SNMP Trap function enabled or not
RMON enable	SNMP RMON enabled or not
Community Information	Information about community string
Trap manager Information	Information about Trap host

Security IP Information	Information about secure IP.

5.4.6.1.3 debug snmp packet

Command: debug snmp packet

no debug snmp packet

Function: Enables the SNMP debug function: the "**no debug snmp packe**t" command disables this debug function.

Command mode: Admin Mode

Usage Guide: When problems occur in SNMP, SNMP debug function can be enabled to locate the cause.

Example:

Switch#debug snmp packet

5.4.6.2 SNMP Troubleshooting Help

In configuring and using SNMP, the SNMP server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ Interface and datalink layer protocol is Up (use the "show interface" command), and the connection between the switch and host are intact and can be verified by ping (use "ping" command).
- ✧ The switch enabled SNMP Agent server function (use "snmp-server enable" command)
- ✧ Secure IP for NMS (use "snmp-server securityip" command) and community string (use "snmp-server community" command) are correctly configured, as if any of them fails, SNMP will not be able to communicate with NMS properly.
- ✧ If Trap function is required, remember to enable Trap (use "snmp-server enable traps" command), and remember to properly configure the target host IP address and community string for Trap (use "snmp-server host" command) to ensure Trap message can be sent to the specified host.
- ✧ If RMON function is required, RMON must be enabled first (use "rmon enable" command).
- ✧ During SNMP operation, if the user has any doubt, "show snmp" command can be used to check for statistics for SNMP traffic, or use "show snmp status" command to check for SNMP configuration information, or "debug snmp packet" command to enable SNMP debugging function and view the debug output.

5.5 Switch Upgrade

ES4704BD provides two ways for switch upgrade: BootROM upgrade and the TFTP/FTP upgrade under Shell.

5.5.1 BootROM Upgrade

There are two methods for BootROM upgrade: TFTP and FTP, which can be selected at BootROM command settings.

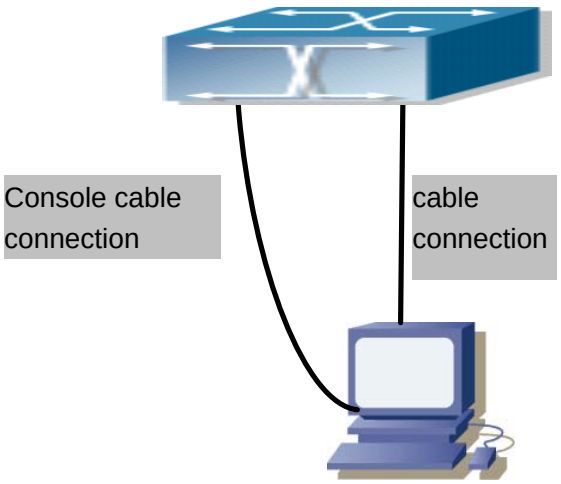


Fig 5-3 Typical topology for switch upgrade in BootROM mode

The upgrade procedures are listed below:

Step 1:

As shown in the figure, a PC is used as the console for the switch. A console cable is used to connect PC to the management port on the switch. The PC should have FTP/TFTP server software installed and have the img file required for the upgrade.

Step 2:

Press “ctrl+b” on switch boot up until the switch enters BootROM monitor mode. The operation result is shown below:

ES4704BD Management Switch

Copyright (c) 2001-2004 by Edge-Core Networks Limited.
All rights reserved.

Reset chassis ... done.
Testing RAM...
134,217,728 RAM OK.

Loading BootROM...
Starting BootRom...
Attaching to file system ... done.
219.32 BogoMIPS
SST39VF040

CPU: PowerPC MPC8245MH266, Revision 14
Version: 1.4.1
Creation date: Apr 14 2005, 09:33:18

Attached TCP/IP interface to lnPci0.
[Boot]:

Step 3:

Under BootROM mode, run "setconfig" to set the IP address and mask of the switch under BootROM mode, server IP address and mask, and select TFTP or FTP upgrade.

For example, suppose the switch address is 192.168.1.2/24, the PC address is 192.168.1.66/24. Select TFTP upgrade. The configuration should like:

[Boot]: setconfig
Host IP Address: 10.1.1.1 192.168.1.2
Server IP Address: 10.1.1.2 192.168.1.66
FTP(1) or TFTP(2): 1 2
Network interface configure OK.
[Boot]:

Step 4:

Enable FTP/TFTP server in the PC. For TFTP, run TFTP server program; for FTP, run FTP server program. Before downloading the upgrade file to the switch, verify the connectivity between the server and the switch by ping from the server. If ping succeeds, run "load" command in the BootROM mode from the switch; if it fails, perform troubleshooting to find out the cause. The following is the configuration for the system update mirror file.

[Boot]: load nos.img
Loading...
entry = 0x10010
size = 0x1077f8

Step 5:

Example: Execute "write nos.img" in BootROM mode. The following saves the system update

mirror file.

[Boot]: write nos.img

Programming...

Program OK.

[Boot]:

Step 6:

After successful upgrade, execute the "run" command in BootROM mode to return to CLI configuration interface.

[Boot]:run（or reboot）

Other commands in BootROM mode

1. DIR command

Used to list existing files in the FLASH.

[Boot]: dir

boot.rom	327,440 1900-01-01 00:00:00 --SH
boot.conf	83 1900-01-01 00:00:00 --SH
nos.img	2,431,631 1980-01-01 00:21:34 ----
startup-config	2,922 1980-01-01 00:09:14 ----
temp.img	2,431,631 1980-01-01 00:00:32 ----

2. CONFIG RUN command

Used to set the IMG file to run upon system start-up, and the configuration file to run upon configuration recovery.

[Boot]: config run

Boot File: [nos.img] nos1.img

Config File: [boot.conf]

5.5.2 FTP/TFTP Upgrade

5.5.2.1 Introduction to FTP/TFTP

FTP (File Transfer Protocol) / TFTP (Trivial File Transfer Protocol) are both file transfer protocols that belonging to layer four (application layer) of the TCP/IP protocol stack, used for transferring files between hosts and between hosts and switches. Both of them transfer files in a client-server model. Their differences are listed below.

FTP builds upon TCP to provide reliable connection-oriented data stream transfer service. However, it does not provide file access authorization and uses simple authentication mechanism(transfers username and password in plain text for authentication). When using FTP to transfer files, two connections need to be established between the client and the server: a management connection and a data connection. A transfer request should be sent by the FTP client

to establish management connection on port 21 in the server, and negotiate a data connection through the management connection.

There are two types of data connections: active connection and passive connection.

In active connection, the client transmits its address and port number for data transmission to the sever, the management connection maintains until data transfer is complete. Then, using the address and port number provided by the client, the server establishes data connection on port 20 (if not engaged) to transfer data; if port 20 is engaged, the server automatically generates some other port number to establish data connection.

In passive connection, the client, through a management connection, notifies the server to establish a passive connection. The server then creates its own data listening port and informs the client about the port, and the client establishes a data connection to the specified port.

As data connection is established through the specified address and port, there is a third party to provide data connection service.

TFTP builds upon UDP, providing unreliable data stream transfer service with no user authentication or permission-based file access authorization. It ensures correct data transmission by sending and acknowledging mechanism and retransmission of time-out packets. The advantage of TFTP over FTP is that it is a simple and low overhead file transfer service.

ES4704BD can operate as either FTP/TFTP client or server. When ES4704BD operates as a FTP/TFTP client, configuration files or system files can be downloaded from the remote FTP/TFTP servers (can be hosts or other switches) without affecting its normal operation. And file list can also be retrieved from the server in ftp client mode. Of course, ES4704BD can also upload current configuration files or system files to the remote FTP/TFTP servers (can be hosts or other switches). When ES4704BD operates as a FTP/TFTP server, it can provide file upload and download service for authorized FTP/TFTP clients, as file list service as FTP server.

Here are some terms frequently used in FTP/TFTP.

ROM: Short for EPROM, erasable read-only memory. EPROM is replaced by FLASH memory in ES4704BD.

SDRAM: RAM memory in the switch, used for system software operation and configuration sequence storage.

FLASH: Flash memory used to save system files and configuration files

System file: including system mirror file and boot file.

System mirror file: refers to the compressed file for switch hardware driver and software support program, usually refer to as IMG upgrade file. In ES4704BD, the system mirror file is allowed to save in FLASH only. ES4704BD mandates the name of system mirror file to be uploaded via FTP in Global Mode to be nos.img, other IMG system files will be rejected.

Boot file: refers to the file that initializes the switch, also referred to as the ROM upgrade file (large-sized file can be compressed as IMG file). In ES4704BD, the boot file is allowed to save in ROM only. ES4704BD mandates the name of the boot file to be boot.rom.

Configuration file: including start up configuration files and active configuration files. The distinction between a start up configuration file and an active configuration file can facilitate the

backup and update of the configurations.

Start up configuration file: refers to the configuration sequence used in switch start up. ES4704BD start up configuration file stores in FLASH only, corresponding to the so called configuration save. To prevent illicit file upload and easier configuration, ES4704BD mandates the name of start up configuration file to be startup-config.

Active configuration file: refers to the active configuration sequence used in the switch. In ES4704BD, the active configuration file is stored in the RAM. In the current version, the active configuration sequence running-config can be saved from the RAM to FLASH by the **write** command or the **copy running-config startup-config** command, so that the active configuration sequence becomes the start up configuration file, which is called configuration save. To prevent illicit file upload and easier configuration, ES4704BD mandates the name of active configuration file to be running-config.

Factory configuration file: The configuration file shipped with ES4704BD is in the name of factory-config. Run **set default, write**, and then restart the switch. The factory configuration file will be loaded to overwrite the current start up configuration file.

5.5.2.2 FTP/TFTP Configuration

The configurations of ES4704BD as FTP and TFTP clients are almost the same, so the configuration procedures for FTP and TFTP are described together in this manual.

5.5.2.2.1 FTP/TFTP Configuration Task Sequence

1. FTP/TFTP client configuration
   （1）Upload/download the configuration file or system file.
   （2）For FTP client, server file list can be checked.
2. FTP server configuration
   （1）Start FTP server
   （2）Configure FTP login username and password
   （3）Modify FTP server connection idle time
   （4）Shut down FTP server
3. TFTP server configuration
   （1）Start TFTP server
   （2）Configure TFTP server connection idle time
   （3）Configure retransmission times before timeout for packets without acknowledgement
   （4）Shut down TFTP server

1. FTP/TFTP client configuration

（1）FTP/TFTP client upload/download file

Command	Explanation

Admin Mode	
copy <***source-url***> <***destination-url***> **[ascii | binary]**	FTP/TFTP client upload/download file

（2）For FTP client, server file list can be checked

Global Mode	
dir <***ftpServerUrl***>	For FTP client, server file list can be checked. *FtpServerUrl* format looks like: ftp://user:password@IP Address

2. FTP server configuration

（1）Start FTP server

Command	Explanation
Global Mode	
ftp-server enable **no ftp-server enable**	Starts FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

（2）Configure FTP login username and password

Command	Explanation
Global Mode	
ip ftp <***username***> **password [type{0|7}]** <***password***> **no ip ftp username** <***username***>	Configures the FTP username and password; the "**no ip ftp username** <***username***>" command deletes the password as well as the username configured.

（3）Modify FTP server connection idle time

Command	Explanation
Global Mode	
ftp-server timeout <***seconds***>	Sets connection idle time

3. TFTP server configuration

（1）Start TFTP server

Command	Explanation
Global Mode	
tftp-server enable **no tftp-server enable**	Starts TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP users from logging in.

（2）Modify TFTP server connection idle time

Command	Explanation

Global Mode	
tftp-server retransmission-number < *number* >	Sets maximum retransmission time within timeout interval.

（3）Modify TFTP server connection retransmission time

Command	Explanation
Global Mode	
tftp-server retransmission-number < *number* >	Set maximum retransmission time within timeout interval.

5.5.2.2.2 FTP/TFTP Configuration Commands

5.5.2.2.3 copy（FTP）

Command: copy <***source-url***> **<*destination-url*> [ascii | binary]**

Function: FTP client upload/download file

Parameters: <***source-url***> is the source file or directory location to be copied; **<*destination-url*>** is the target address to copy file or directory; <***source-url***> and **<*destination-url*>** varies according to the file or directory location. **ascii** indicates the files are transferred in ASCII; **binary** indicates the files are transferred in binary (default). The URL format for FTP address looks like: ftp://<*username*>:<*password*>@<*ipaddress*>/<*filename*>, where <*username*> is the FTP username, <*password*> is the FTP user password, <*ipaddress*> is the IP address of FTP server/client; <*filename*> is the name of the file to be uploaded/downloaded via FTP.

Special Keywords in filename

keyword	**Source/Target IP address**
running-config	Active configuration file
startup-config	Start up configuration file
nos.img	System file
Boot.rom	System boot file

Command mode: Admin Mode

Usage Guide: The command provides command line prompt messages. If the user enters a command like **copy <*filename*> ftp://** or **copy ftp:// <*filename*>** and presses Enter, the following prompt will appear:

ftp server ip address [x.x.x.x] :

ftp username>

ftp password>

ftp filename>

This prompts for the FTP server address, username, password and file name.

Example:

（1）Saving the mirror in FLASH to FTP server 10.1.1.1, the login username for the FTP server is "Switch", and the password is "edgecore".

Switch#copy nos.img ftp://Switch:edgecore@10.1.1.1/nos.img

（2）Get the system file nos.img from FTP server 10.1.1.1, the login username for the FTP server is "Switch", and the password is "edgecore".

Switch#copy ftp://Switch:edgecore@10.1.1.1/nos.img nos.img

（3）Save active configuration file:

Switch#copy running-config startup-config

Related command: write

5.5.2.2.4 dir

Command: dir <*ftp-server-url*>

Function: checks the list for files in the FTP server

Parameters: < *ftp-server-url* > takes the following format:

ftp://<*username*>:<*password*>@<*ipaddress*>, where <*username*> is the FTP username, <*password*> is the FTP user password, <*ipaddress*> is the IP address of FTP server.

Command mode: Global Mode

Example: viewing the file list of the FTP server 10.1.1.1 with the username "Switch" and password "edgecore".

Switch#config

Switch(Config)#dir ftp:// Switch:edgecore@10.1.1.1

5.5.2.2.5 ftp-server enable

Command: ftp-server enable

no ftp-server enable

Function: Enables FTP server, the "**no ftp-server enable**" command shuts down FTP server and prevents FTP user from logging in.

Default: FTP server is not enabled by default.

Command mode: Global Mode

Usage Guide: When FTP server function is enabled, the switch can still perform ftp client functions. FTP server is not enabled by default.

Example: enable FTP server service.

Switch#config

Switch(Config)# ftp-server enable

Related command: ip ftp

5.5.2.2.6 ftp-server timeout

Command: ftp-server timeout <*seconds*>

Function: Sets the data connection idle time

Parameters: <*seconds*> is the idle time threshold (in seconds) for a FTP connection, the valid range is 5 to 3600.

Default: The system default is 600 seconds.

Command mode: Global Mode

Usage Guide: When FTP data connection idle time exceeds this limit, the FTP management connection will be disconnected.

Example: Modify the idle threshold to 100 seconds.

Switch#config

Switch(Config)#ftp-server timeout 100

5.5.2.2.7 ip ftp

Command:ip ftp <*username*> password [type{0|7}] <*password*>

no ip ftp username <*username*>

Function: Configures the FTP username and password; the "**no ip ftp username <*username*>**" command deletes the password as well as the username configured.

Parameters: <*username*> is the FTP connection username, up to 16 characters are allowed; 0|7 indicates non-masked password display and masked password display; **<*password*>** is the FTP connection password, up to 16 characters are allowed.

Default: Anonymous FTP connection is used by default.

Command mode: Global Mode

Example: configuring the username to be "ECSwitch", and password to be "edgecore".

Switch#

Switch#config

Switch(Config)#ip ftp ECSwitch password 0 edgecore

Switch(Config)#

5.5.2.2.8 copy（TFTP）

Command: copy <*source-url*> <*destination-url*> [ascii | binary]

Function: TFTP client upload/download file

Parameters: <***source-url***> is the source file or directory location to be copied; <***destination-url***> is the target address to copy file or directory; <***source-url***> and <***destination-url***> varies according to the file or directory location. **ascii** Indicates the files are transferred in ASCII; **binary** indicates the files are transferred in binary (default) The URL format for TFTP address looks like: tftp://<*ipaddress*>/<*filename*>, where <*ipaddress*> is the IP address of TFTP server/client, <*filename*> is the name of the file to be uploaded/downloaded via TFTP.

Special Keywords in filename

Keyword	**Source/Target IP address**
running-config	Active configuration file
startup-config	Start up configuration file
nos.img	System file
Boot.rom	**System boot file**

Command mode: Admin Mode

Usage Guide: The command provides command line prompt messages. If the user enters a command like **copy <*filename*> tftp://** or **copy tftp:// <*filename*>** and presses Enter, the following prompt will appear:

tftp server ip address>

tftp filename>

This prompts for the TFTP server address and file name.

Example:

（1）Saving the mirror in FLASH to TFTP server 10.1.1.1:

Switch#copy nos.img tftp:// 10.1.1.1/ nos.img

（2）Getting the system file nos.img from TFTP server 10.1.1.1:

Switch#copy tftp://10.1.1.1/nos.img nos.img

（3）Saving the active configuration file:

Switch#copy running-config startup-config

Related command: write

5.5.2.2.9 tftp-server enable

Command: tftp-server enable

no tftp-server enable

Function: Starts TFTP server, the "**no ftp-server enable**" command shuts down TFTP server and prevents TFTP user from logging in.

Default: TFTP server is not started by default.

Command mode: Global Mode

Usage Guide: When the TFTP server function is enabled, the switch can still perform tftp client

functions. TFTP server is not started by default.

Example: Enabling the TFTP server service.

Switch#config

Switch(Config)#tftp-server enable

Related command: tftp-server timeout

5.5.2.2.10 tftp-server retransmission-number

Command: tftp-server retransmission-number <*number*>

Function: Sets the retransmission time for TFTP server

Parameters: < *number*> is the time to re-transfer, the valid range is 1 to 20.

Default: The default value is 5 retransmission.

Command mode: Global Mode

Example: Modifying the retransmission time to 10 times.

Switch#config

Switch(Config)#tftp-server retransmission-number 10

5.5.2.2.11 tftp-server transmission-timeout

Command: tftp-server transmission-timeout <*seconds*>

Function: Sets the transmission timeout value for the TFTP server

Parameters: <*seconds*> is the timeout value, the valid range is 5 to 3600 seconds..

Default: The system default timeout setting is 600 seconds.

Command mode: Global Mode

Example: Modifying the timeout value to 60 seconds.

Switch#config

Switch(Config)#tftp-server transmission-timeout 60

5.5.2.3 FTP/TFTP Configuration Examples

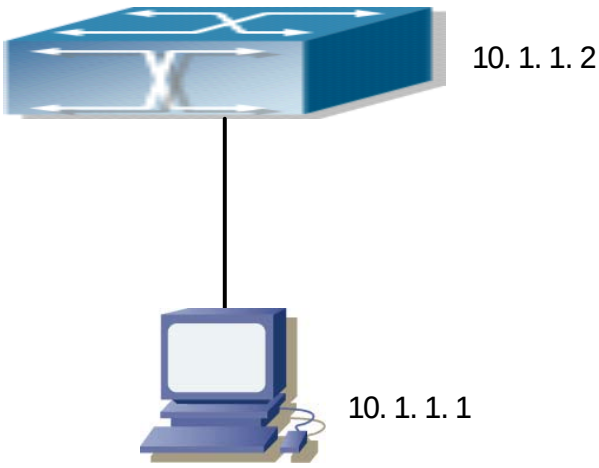


Fig -5-4 Download nos.img file as FTP/TFTP client

Scenario 1: The switch is used as FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; the switch acts as a FTP/TFTP client, the IP address of the switch management VLAN is 10.1.1.2. Download "nos.img" file in the computer to the switch.

■ **FTP Configuration**

Computer side configuration:

Start the FTP server software on the computer and set the username as "Switch", and the password as "edgecore". Place the "12_30_nos.img" file in the appropriate FTP server directory on the computer.

The configuration procedures of the switch are listed below:

Switch(Config)#inter vlan 1

Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0

Switch (Config-If-Vlan1)#no shut

Switch (Config-If-Vlan1)#exit

Switch (Config)#exit

Switch#copy ftp://Switch:edgecore@10.1.1.1/12_30_nos.img nos.img

With the above commands, the switch will have the "nos.img" file in the computer downloaded to the FLASH.

■ **TFTP Configuration**

Computer side configuration:

Start TFTP server software on the computer and place the "nos.img" file to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch is listed below:

Switch (Config)#inter vlan 1

Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy tftp://10.1.1.1/12_30_nos.img nos.img

Scenario 2: The switch is used as a FTP server. The switch operates as the FTP server and connects from one of its ports to a computer, which is a FTP client. Transfer the "nos.img" file in the switch to the computer and save as 12_25_nos.img.
The configuration procedures of the switch are listed below:
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#ftp-server enable
Switch(Config)#ip ftp Switch password 0 edgecore

Computer side configuration:
Log in to the switch with any FTP client software, with the username "Switch" and password "edgecore", use the command "get nos.img 12_25_nos.img" to download the "nos.img" file from the switch to the computer.

Scenario 3: The switch is used as TFTP server. The switch operates as the TFTP server and connects from one of its ports to a computer, which is a TFTP client. Transfer the "nos.img" file in the switch to the computer.
The configuration procedures of the switch are listed below:
Switch(Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#tftp-server enable
Computer side configuration:
Log in to the switch with any TFTP client software, use the "tftp" command to download the "nos.img" file from the switch to the computer.

Scenario 4: The switch is used as a FTP/TFTP client. The switch connects from one of its ports to a computer, which is a FTP/TFTP server with an IP address of 10.1.1.1; several switch user profile configuration files are saved in the computer. The switch operates as the FTP/TFTP client, the

management VLAN IP address is 10.1.1.2. Download the switch user profile configuration files from the computer to the switch's FLASH.

- **FTP Configuration**

Computer side configuration:

Start the FTP server software on the computer and set the username as "Switch", and the password as "edgecore". Save "Profile1", "Profile2" and "Profile3" in the appropriate FTP server directory on the computer.

The configuration procedures of the switch are listed below:

```
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy ftp://Switch:edgecore@10.1.1.1/Profile1 Profile1
Switch#copy ftp://Switch:edgecore@10.1.1.1/Profile2 Profile2
Switch#copy ftp://Switch:edgecore@10.1.1.1/Profile3 Profile3
```

With the above commands, the switch will have the user profile configuration file in the computer downloaded to the FLASH.

- **TFTP Configuration**

Computer side configuration:

Start TFTP server software on the computer and place "Profile1", "Profile2" and "Profile3" to the appropriate TFTP server directory on the computer.

The configuration procedures of the switch are listed below:

```
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#exit
Switch#copy tftp://10.1.1.1/ Profile1 Profile1
Switch#copy tftp://10.1.1.1/ Profile2 Profile2
Switch#copy tftp://10.1.1.1/ Profile3 Profile3
```

Scenario 5: ES4704BD acts as FTP client to view file list on the FTP server.

Synchronization conditions: The switch connects to a computer by a Ethernet port, the computer is a FTP server with an IP address of 10.1.1.1; the switch acts as a FTP client, and the IP address of the switch management VLAN1 interface is 10.1.1.2.

FTP Configuration

PC side:

Start the FTP server software on the PC and set the username as “Switch”, and the password as “edgecore”.

ES4704BD：

```
Switch (Config)#inter vlan 1
Switch (Config-If-Vlan1)#ip address 10.1.1.2 255.255.255.0
Switch (Config-If-Vlan1)#no shut
Switch (Config-If-Vlan1)#exit
Switch (Config)#dir ftp://Switch:edgecore@10.1.1.1
220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
150 Opening ASCII mode data connection for /bin/ls.
recv total = 480
nos.img
nos.rom
parsecommandline.cpp
position.doc
qmdict.zip
shell maintenance statistics.xls
… (some display omitted here)
show.txt
snmp.TXT
226 Transfer complete.
Switch (Config)#
```

5.5.2.4 FTP/TFTP Troubleshooting Help

5.5.2.4.1 Monitor and Debug Commands

5.5.2.4.2 show ftp

Command: show ftp

Function: display the parameter settings for the FTP server

Command mode: Admin Mode

Default: No display by default.

Example:

Switch#show ftp
Timeout :600

Displayed information	Description
Timeout	Timeout time.

5.5.2.4.3 show tftp

Command: show tftp
Function: displays the parameter settings for the TFTP server
Default: There is no display by default.
Command mode: Admin Mode
Example:
Switch#show tftp
timeout :60
Retry Times :10

Displayed information	Explanation
Timeout	Timeout time
Retry Times	Retransmission times

5.5.2.4.4 FTP Troubleshooting Help

When uploading/downloading system files with FTP protocol, the connectivity of the link must be ensured, i.e., use the "**ping**" command to verify the connectivity between the FTP client and server before running the FTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

☞ The following is what the message displays when files are successfully transferred. Otherwise, please verify link connectivity and retry the "copy" command again.

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
nos.img file length = 1526021
read file ok
send file
150 Opening ASCII mode data connection for nos.img.
226 Transfer complete.
close ftp client.

- ☞ The following is the message displays when files are successfully received. Otherwise, please verify link connectivity and retry “copy” command again.

220 Serv-U FTP-Server v2.5 build 6 for WinSock ready...
331 User name okay, need password.
230 User logged in, proceed.
200 PORT Command successful.
recv total = 1526037
****
write ok
150 Opening ASCII mode data connection for nos.img (1526037 bytes).
226 Transfer complete.

- ☞ If the switch is upgrading a system file or the system start up file through FTP, the switch must not be restarted until “close ftp client” or “226 Transfer complete” is displayed, indicating the upgrade was successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through FTP fails, please try to upgrade again or use the BootROM mode to upgrade.

5.5.2.4.5 TFTP Troubleshooting Help

When upload/download system file with TFTP protocol, the connectivity of the link must be ensured, i.e., use the “**ping**” command to verify the connectivity between the TFTP client and server before running the TFTP program. If ping fails, you will need to check for appropriate troubleshooting information to recover the link connectivity.

- ☞ The following is the message displayed when files are successfully transferred. Otherwise, please verify link connectivity and retry “copy” command again.

  nos.img file length = 1526021
  read file ok
  begin to send file,wait...
  file transfers complete.
  close tftp client.

- ☞ The following is the message displayed when files are successfully received. Otherwise, please verify link connectivity and retry the “copy” command again.

  begin to receive file,wait...
  recv 1526037
  ****
  write ok
  transfer complete
  close tftp client.

If the switch is upgrading system file or system start up file through TFTP, the switch must not be restarted until "close tftp client" is displayed, indicating upgrade is successful, otherwise the switch may be rendered unable to start. If the system file and system start up file upgrade through TFTP fails, please try to upgrade again or use the BootROM mode to upgrade.

5.6 WEB MANAGEMENT

5.6.1 Switch basic configuration

Users should click "Switch basic configuration" table and configure the switch's clock, prompts of command-line interface, timeout of quitting privileged configuration mode, etc.

5.6.1.1 Basicconfig

Users should click "Switch basic configuration" and "BasicConfig" to configure the switch's clock, prompts of command-line interface and the mapping address relationship with the host.

Basic clock configuration – configure "date and clock" of the system. Please refer to the CLI command 5.1.1.

Users should configure HH:MM:SS as 23:0:0 and YY.MM.DD as 2002/08/01. The complete configuration by clicking on the "Apply" button.

- Hostname configuration – configures prompts of command-line interface. Please refer to the CLI command 5.1.9.

Example: configure the Hostname as "Test" and then click on the "Apply" button to apply this configuration to the switch.

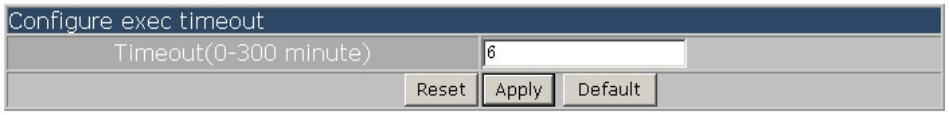
- Basic host configuration – configures the mapping relationship between the switch and the IP address. Please refer to the CLI command 5.1.8.

Example: configure the Hostname as "London" and IP address as 200.121.1.1 and then click on the "Apply" button. This configuration will be applied to the switch.

Users should click "Switch basic configuration" and "Configure exec timeout" to configure the timeout of quitting privileged configuration mode. Please refer to the CLI command 5.1.5.

5.6.1.2 Configure exec timeout

Example of configuring the timeout as 6 minutes and then click on the "Apply" button to complete the timeout of quitting privileged configuration mode.



5.6.2 SNMP configuration

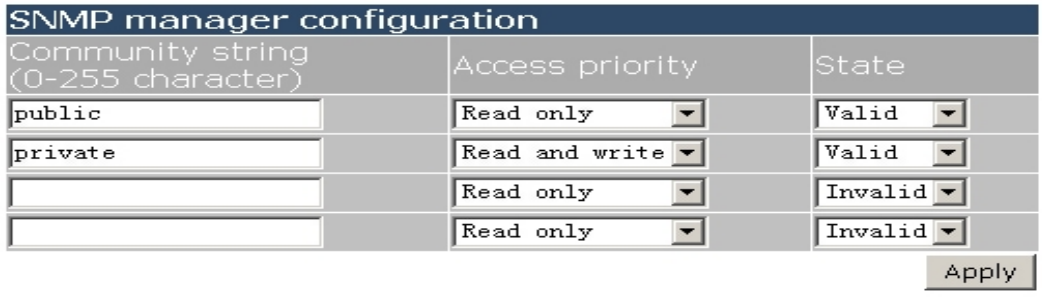
Users should click "Switch basic configuration" and "SNMP configuration" to configure the SNMP relating functions.

5.6.2.1 SNMP manager configuration

Users should click "Switch basic configuration", "SNMP configuration", and "SNMP manager configuration" to configure the community string of the switch. Please refer to the CLI command 5.4.4.2.2.

- Community string (0-255 characters) – for configuration of the community string.
- Access priority – specifies access rights to MIB, including "Read only" and "Read and write."
- State – "Valid" – to configure; "Invalid" – to remove.

Users should configure Community string as "public", choose Access priority as "Read only" mode, and choose State as "Valid" or configure Community string as private, choose Access priority as "Read and write" mode, and choose State as "Valid". The command will be applied to the switch by clicking on the "Apply" button.

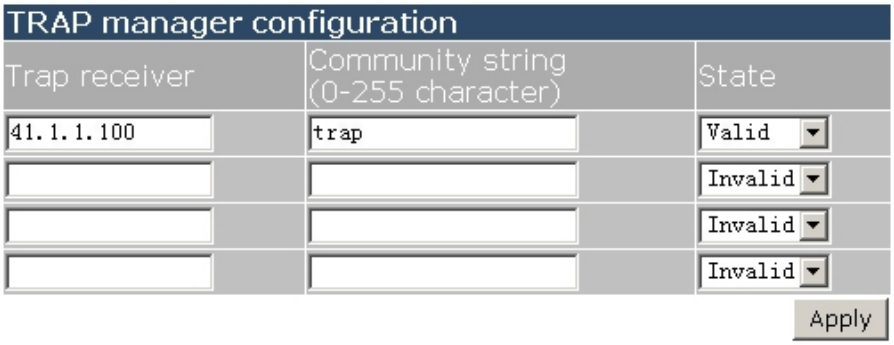


5.6.2.2 Trap manager configuration

Users should click "Switch basic configuration", "SNMP configuration", and "TRAP manager configuration" to configure the IP address of the management station which will receive SNMP Trap messages and Trap community strings. Please refer to the CLI command 5.4.4.2.5.

- Trap receiver – the IP address of NMS management station that will receive Trap messages.
- Community string (0-255 character) – the community string used to send Trap messages.
- State – "Valid" – to configure; "Invalid" – to remove

Example: configure the Trap receiver as "41.1.1.100" and configure the community string as "trap" and State as "Valid." The command will be applied to the switch by clicking on the "Apply" button.

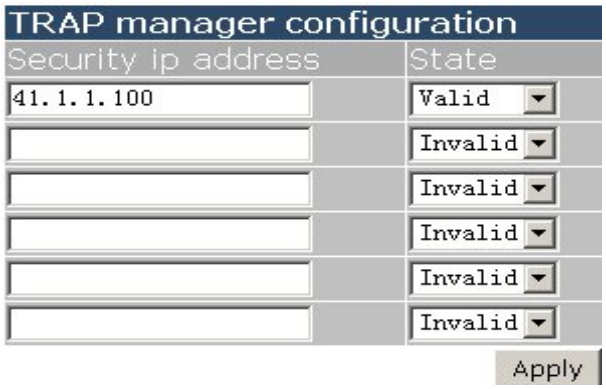


5.6.2.3 Configure IP address of SNMP manager

User should click "Switch basic configuration", "SNMP configuration", and "Configure ip address of snmp manager" to configure the security IP address which will be allowed to access to the NMS management station of the switch. Please refer to the CLI command 5.4.4.2.6.

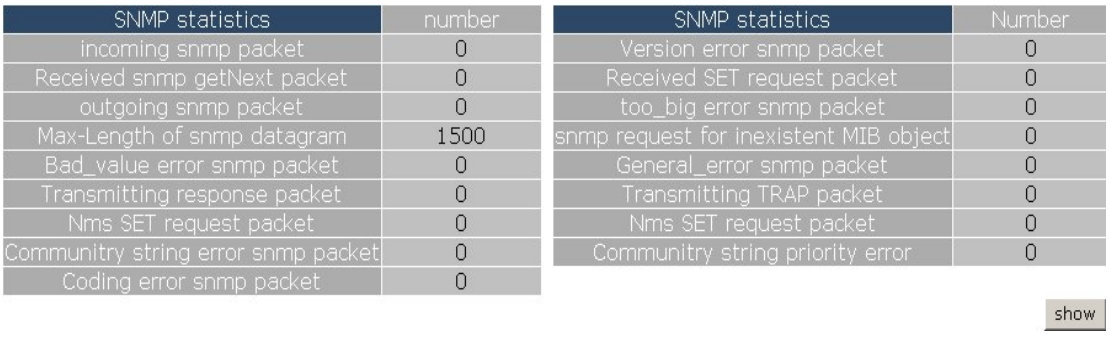
- Security ip address – Security IP address of NMS
- State –"Valid" – to configure; "Invalid" – to remove

Example: configure the security IP address as "41.1.1.100", and choose State as "Valid". The command will be applied to the switch by clicking on the "Apply" button.



5.6.2.4 SNMP statistics

When users click "Switch basic configuration", "SNMP configuration" and "SNMP statistics", a variety of counter information will appear. Please refer to the CLI command 5.4.6.1.1.

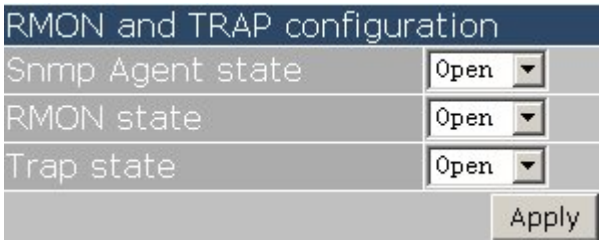


5.6.2.5 RMON and trap configuration

Users should click "Switch basic configuration", "SNMP configuration" and "RMON and TRAP configuration" to configure the RMON function of the switch.

- Snmp Agent state –open/close the switch to be SNMP agent server function. Please refer to the CLI command 5.4.4.2.3.
- RMON state – open/close RMON function of the switch. Please refer to the CLI command 5.4.4.2.1.
- Trap state – allows device to send Trap messages, Please refer to the CLI command 5.4.4.2.4

Example: choose Snmp Agent state as "Open", choose RMON state as "Open", and choose Trap state as "Open". Then click on the "Apply" button.



5.6.3 Switch upgrade

Users should click "Switch basic configuration" and "Switch update" to configure the upgrade Node Tree Diagram. Two categories are explained below:

- TFTP Upgrade, including
  - ✓ TFTP client service – to configure TFTP client
  - ✓ TFTP server service – to configure TFTP server
- FTP Upgrade, including
  - ✓ FTP client service – to configure FTP client
  - ✓ FTP server service – to configure FTP server

5.6.3.1 TFTP client configuration

Users should click "Switch basic configuration" and "TFTP client service" to enter into the configuration page. Please refer to the CLI command 5.5.2.2.9.

Words and phrases are explained in the following:

Server IP address－IP address of the server.

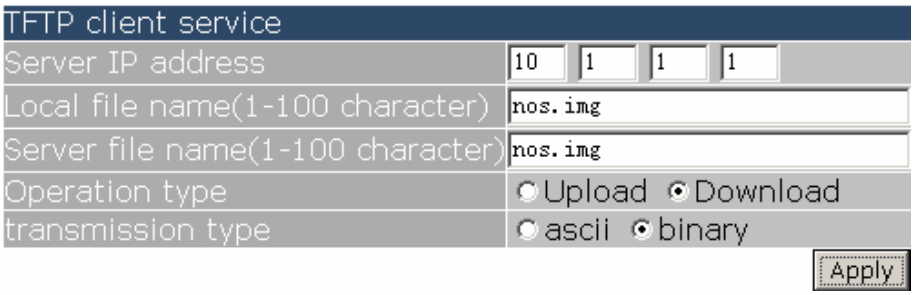
Local file name－the local file name

Server file name－the file name of the server

Operation type－"Upload" means to upload files; "Download" means to download files

Transmission type－"ascii" means to transit files by using ASCII standard. "binary" means the files are transmitted in the binary standard

Example: the Figure below shows how to get the system file from TFTP Server 10.1.1.1, which has server file name is "nos.img" and local file name "nos.img." Click "Apply" to finish.



5.6.3.2 TFTP server configuration

Users should click "Switch basic configuration" and "TFTP server service" to enter into the configuration page.

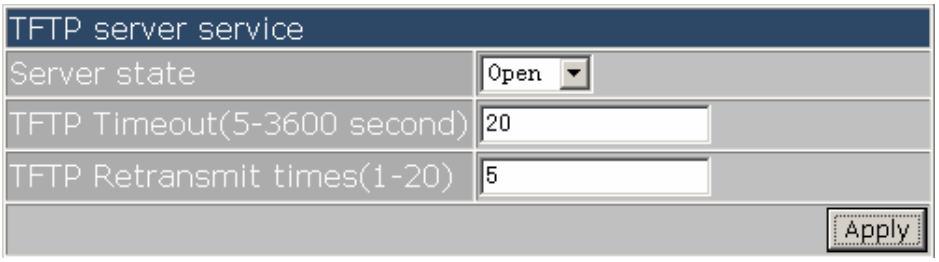
Words and phrases are explained in the following:

Server state－status of the server. ("Open" or "Close") Please refer to the CLI command 5.5.2.2.10

TFTP Timeout－the timeout. Please refer to the CLI command 5.5.2.2.12.

TFTP Retransmit times－times of retransmission. Please refer to the CLI command 5.5.2.2.11.

Users should open the TFTP server, and choose "Open" and then click "Apply."



5.6.3.3 FTP client configuration

Users should click "Switch basic configuration" and "FTP client service" to enter into this configuration page. Please refer to the CLI command 5.5.2.2.3。

Words and phrases are explained in the following:

Server IP address－IP address of the server

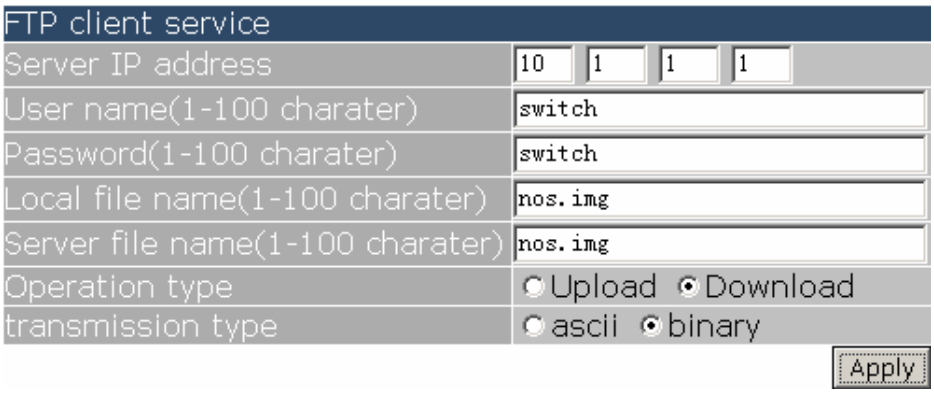
User name－the name of the user

Password－the specific password

Operation type－"Upload" means to upload files; "Download" means to download files

Transmission type－"ascii" means to transit files by using ASCII standard. "binary" means the files are transmitted in binary standard.

Users should follow the Figure below to get the system file from the FTP Server 10.1.1.1, with server file name is "nos.img" and local file name "nos.img." The ftp username is "switch" and password is "switch". Click "Apply".



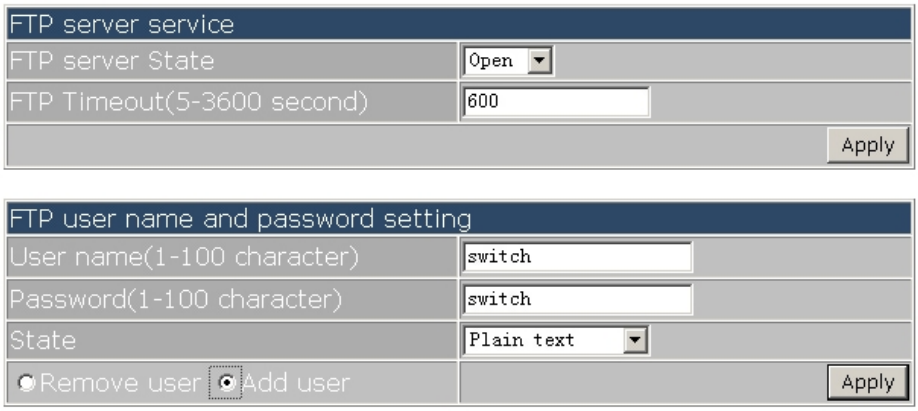
5.6.3.4 FTP server configuration

Users should click "Switch basic configuration" and "FTP server service" to enter into the configuration page and make configuration nodes, which include "server configuration" and "user configuration."

Words and phrases of "user configuration" are explained in the following:

- FTP Server state—status of the server. ("Open" or "Close".) Please refer to the CLI command 5.5.2.2.5.
- FTP Timeout—the timeout. Please refer to the CLI command 5.5.2.2.6.
- User name—the name of the user. Please refer to the CLI command 5.5.2.2.8.
- Password—the specific password. Please refer to the CLI command 5.5.2.2.7.
- State—display the status of the password. "Plain text" means proclaimed display and "encrypted" means "encrypted" display. Please refer to the CLI command 5.5.2.2.7.
- Remove user—to remove a user. Please refer to the CLI command 5.5.2.2.8.
- Add user—to add a user. Please refer to the CLI command 5.5.2.2.8.

Example: open the TFTP server, input the username "switch" and password "switch", and then click "Apply."



5.6.4 Maintenance and debug command

Users should click "Switch basic configuration" and "Basic configuration debug" to enter into the configuration page and make configuration nodes, which include the following segments:

- Debug command—a debugging command.
- Show clock—to display the current time. Please refer to the CLI command 5.2.4.1.

- Show flash－to display FLASH files. Please refer to the CLI command 5.2.4.3.
- Show history－to display the latest inputted commands. Please refer to the CLI command 5.2.4.4.
- Show running-config－to display the current status of parameters configuration. Please refer to the CLI command 5.2.4.6.
- Show switch port interface－to display properties of VLAN ports. Please refer to the CLI command 5.2.4.8.
- Show tcp－to display the current TCP connection with the switch. Please refer to the CLI command 5.2.4.9.
- Show udp－to display the current UDP connection with the switch. Please refer to the CLI command 5.2.4.10.
- Show telnet login－to display the Telnet client messages connected through Telnet with the switch. Please refer to the CLI command 5.2.4.11.
- Show telnet user－to display all Telnet client messages with authenticated switch access through Telnet. Please refer to the CLI command 5.2.4.12.
- Show version－to display the number/version of the switch. Please refer to the CLI command 5.2.4.13.

5.6.4.1 Debug command

User should click “Switch basic configuration”, “Basic configuration debug”, and “Debug command” to enter into the configuration page and make configuration nodes, which include “ping” and “traceroute” segments. They are individually of the same CLI command as 5.2.1 and 5.2.3.

Words and phrases of “Ping” segment are explained in the following:

IP address－the destination IP address

Hostname－the name of the host Words and phrases of “IP Traceroute” segment are explained in the following:

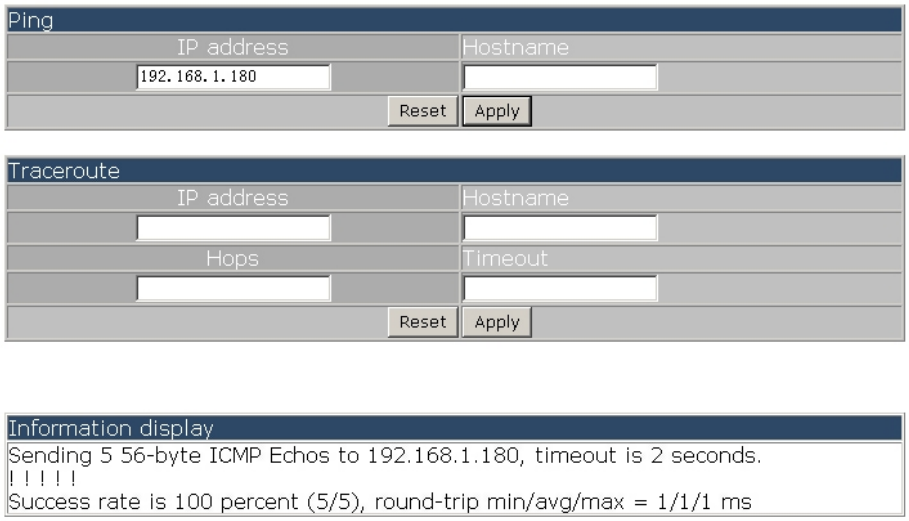
IP address－the destination IP address

Hostname－the name of the host

Hops－the maximum passing hops

Timeout－ the timeout of data packets

Example: “ping” 192.168.1.180 and then click “Apply.”

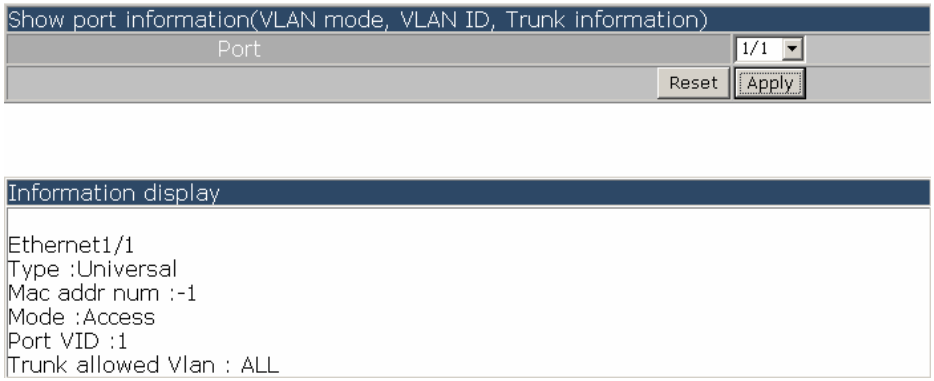


5.6.4.2 Show vlan port property

Users should click “Switch basic configuration”, “Basic configuration debug” and “show switchport interface” to enter into the configuration page and make configuration nodes. Please refer to the CLI command 5.2.4.8.

“Port” means the port table.

Example: User finds a VLAN port’s properties by choosing port1/1 and click “Apply.”

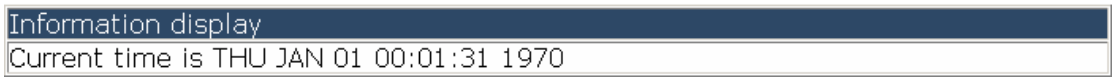


5.6.4.3 Others

Other parts are easier to configure. Users just click a configuration node and the relating messages will appear.

Example:

to display the clock:



to display FLASH files:

Information display	
boot.rom	341,748 1900-01-01 00:00:00 --SH
boot.conf	76 1900-01-01 00:00:00 --SH
nos.img	2,911,216 2005-09-14 14:21:26 ----
nos.pkg	2,911,216 2005-09-12 10:24:34 ----
startup-config	383 2005-11-23 15:24:18 ----
Total 6164639&nbs	

5.6.5 Basic introduction to switch

Users should click "Switch basic configuration" and "Switch basic information" to enter into the configuration page and make configuration nodes

Words and phrases are explained in the following:

- Device type—type of device
- Software version—the number/version of software
- Hardware version—the number/version of hardware
- Prompt—prompts of command-line interface

Switch basic information	
Device type	ES4704BD
software version	2.3.9.0
Hardware version	1.1
prompt	ES4704BD

5.6.6 Switch on-off information

Users should click "Switch on-off information" to enter into the configuration page and make configuration nodes.

Words and phrases are explained in the following:

RIP Status—on-off switch of RIP. ("Open" or "Close") Refer to the CLI command 18.3.2.2.17.

IGMP Snooping—on-off switch of IGMP Snooping. ("Open" or "Close") Refer to the CLI command 11.2.2.1.

Switch GVRP Status—on-off switch of GVRP. ("Open" or "Close") Refer to the CLI command 9.3.2.5.

Example: open IGMP Snooping and close RIP and GVRP, and then click on the "Apply" button.

Switch on-off configuration	
RIP Status	Close
IGMP Snooping	Open
switch GVRP Status	Close

Apply

5.6.7 Switch Maintenance

On the left directory of the root page, users should click "Switch maintenance" to configure

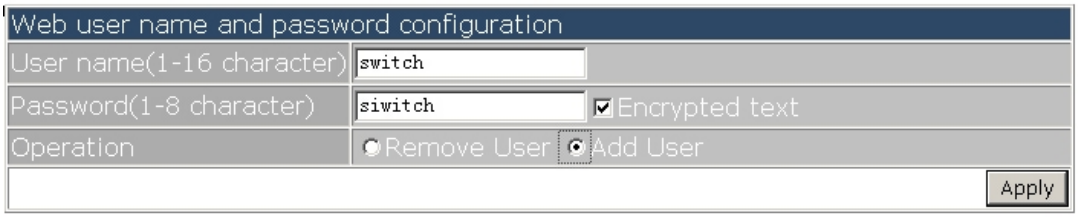
maintenance nodes through web interface.

5.6.7.1 Web server user configuration

Users should click "Switch maintenance", "Web server user configuration" to configure web-user information. Words and phrases are explained in the following:

- User name—to configure a specific name of the web user
- Password—to configure a specific password
- Encrypted text—to configure whether the password is encrypted when displaying configuration information.
- Operation—includes "Remove user" and "Add user"

Example: set the web user name as "switch" and the password as "switch" and then click on the "Apply" button.



5.6.7.2 Exit current web configuration

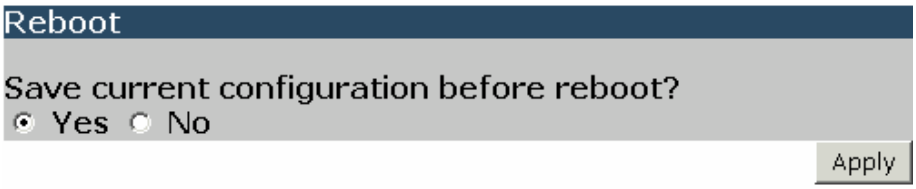
Users should quit the web-login by clicking "Switch maintenance" and "Exit current web configuration."

5.6.7.3 Save current running-config

Users should save the current running-config by clicking "Switch maintenance", "Save current running-config" and "Apply". Please refer to the CLI command 5.1.14.

5.6.7.4 Reboot

Users should reboot the switch by clicking "Switch maintenance." Please refer to the CLI command 5.1.10.



5.6.7.5 Reboot with the default configuration

Users should clear all current configurations and reboot the switch again by clicking "Switch

maintenance" and "Reboot with the default configuration."

5.6.8 Telnet server configuration

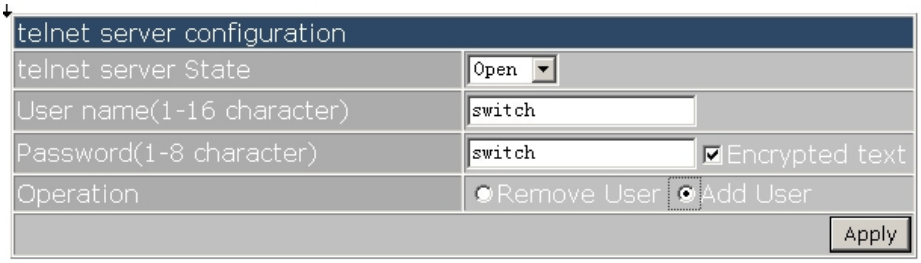
On the left directory of the root page, users may click "Telnet server configuration" and configure the Telnet server configuration nodes through web interface.

5.6.8.1 Telnet server user configuration

Users should click "Telnet server configuration" and "Telnet server user configuration" to configure Telnet service start-up and users information. Please refer to the CLI command 5.2.2.3.3 and 5.2.2.3.5. Words and phrases are explained in the following:

- Telnet server State—to choose from the drop-down list. ("Open" and "Close" service) Please refer to the CLI command 5.2.2.3.3.
  - User name—a specific name of the Telnet user
  - Password—to configure a specific password
  - Encrypted text—to configure whether the password is encrypted when displaying configuration information.
  - Operation—includes "Remove user" and "Add user"

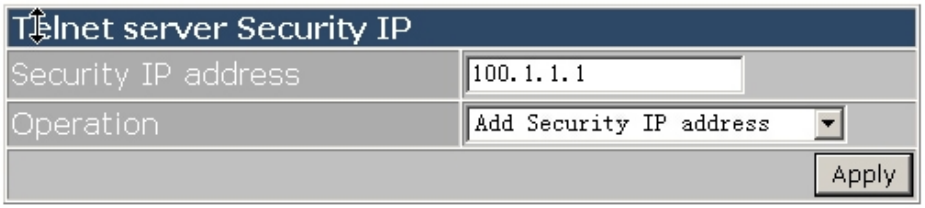
Example: set the Telnet user name as "switch" and password as "switch" and then click on the "Apply" button.



5.6.8.2 Telnet security IP

- Users should click "Telnet server configuration" and "Telnet security IP" to configure the security IP address of an allowed Telnet client for when the switch functions as the Telnet server. Please refer to the CLI command 5.2.2.3.4. Words and phrases are explained in the following:
- Security IP address—a specific security IP address
- Operation—to choose from the drop-down list. ("Add Security IP address" and "Remove Security IP address")

- Example: set "security ip" as "100.1.1.1" to the switch and then click on "Apply".


Telnet server Security IP
Security IP address
100.1.1.1
Operation
Add Security IP address
Apply

Chapter 6 Device Management

6.1 Device Management Brief

The device management function of ES4704BD provides information about line card status, line card operation debugging, power supply and fan status. This function enables the maintenance and management of the physical devices and restart of the switch and line cards, and hot swapping of the cards. ES4704BD supports dual-master mode. If 2 master control boards are present in the system, the master control board in the smaller slot number becomes the Active Master and the other board becomes the Standby Master.

6.2 Device Management Configuration

6.2.1 Switch Basic Configuration

Command: reset slot <*slotno*>

Function: Resets specified card.

Parameters: < ***slotno***> is the slot number, or the card located in that slot, the valid range is 1 to 4, M1, M2, and 5 to 8.

Command mode: Admin Mode

Usage Guide: This command can reset all line cards and Standby Master board, but not the Active Master board.

6.2.2 Device Management Troubleshooting Help

6.2.2.1 Monitor and Debug Commands

6.2.2.1.1 show slot

Command: show slot [<*slotno*>]

Function: to display basic information of every module

Parameter: <***slotno***> is the number of the slot (The range value:1～4)

Default: if slotno does not specify any, then the default displays all of the module information.

Command mode: privileged user configuration mode

Example：

Switch# show slot 1

--------slot : 1--------

Inserted: YES

slot type is: EM4704BD-M12GX-SFP

work mode: active master

work state: RUNNING
software version is: RW-1.3.2
hardware version is: 1.1
bootrom version is: 1.3.1
serialNo is: N043900039
manufactureDate is: 2004/09/10
temperature is: 33.4375

6.2.2.1.2 show fan

Command: show fan

Function to display whether the fan exists or not

Parameter: None

Default: not display

Command mode: privileged user configuration mode

Instructions: ”Inserted” means whether the fan exists or not. One fan tray contains four fans.

Example:

Switch# show fan

----------fan information----------

fan board Inserted: OK

6.2.2.1.3 show power

Command: show power

Function: to display whether the power exists or not

Parameter: None

Default: not display

Command mode: privileged user configuration mode

Instructions: “OK” means the power exits. “NO” means the power does not exist.

Example：

Switch# show power

----------power information----------

power1 Inserted: OK

power2 Inserted: NO

6.2.2.1.4 debug devsm

Command: debug devsm { ***send*** **|** ***receive*** **|** ***state*** }

no debug devsm {***send*** **|** ***receive*** **|** ***state*** }

Function: Displays the device management packet traffic and cards status conditions. The "**no debug devsm** {***send*** **|** ***receive*** **|** ***state*** }" command disables DEBUG display.

Parameters: send displays outgoing device management packets.

receive displays incoming device management packets.

state displays card status change information

Default: Debugging information is disabled by default.

Command mode: Admin Mode

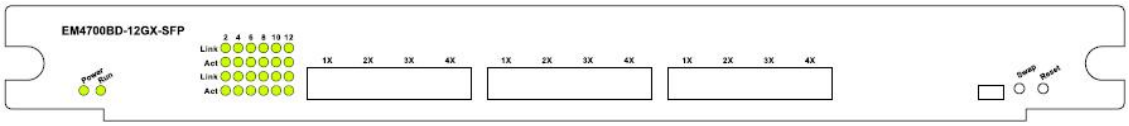
6.3 Card Hot-Swap Operation

ES4704BD supports hot swapping of cards. Hot swapping of non-master control boards/cards will not affect the normal operation of other line cards.

6.3.1 Card Hot-Insertion

The cards are automatically powered once inserted into the slots. A blinking RUN indicator in 1Hz indicates the card is working normally. User entry recognition by the switch will be stopped during the hot insertion of cards and resumed once the cards enter normal operation mode.

6.3.2 Card Hot-Remove



If the cards need to be replaced during normal operation, the following guidelines should be followed:

- Display a message of processing card hot removal.
- The card can be removed when the RUN indicator for the card to be removed goes off and the status of the card in master control board is REMOVED.
- Remove the card, the master control board will indicate the card has been removed (the message displayed on the panel is EMPTY).

Note: Active Master control board can not be removed online.

6.3.3 Configuration Recover Rules

When the switch starts up, the system will reload the information saved in the "StartUp-Config" configuration file from the FLASH. If the card in slot N mismatches the card type saved in "StartUp-Config", then the configuration for that card will not be reloaded.

When the system is operating normally and a user removes a card, the system keeps all the information configured for that card but won't write to FLASH, the information will be lost upon system restart.

When the system is operating normally and the user hot-inserts a card into a slot with a different card inserted previously, the system will not reload configuration; if the slot has a same type of card as the one inserted previously, then the system will try to reload the saved card's configuration; if the saved card's configuration is empty, the slot configuration information recorded in "StartUp-Config" configuration file will be loaded.

6.3.4 Active-Standby Alternation

The switch supports Active-Standby alternation, i.e., when master control boards are present and working normally, the user can switch the master control board role between Active Master and Standby Master. The "show slot" command can be used to determine the Active Master, non-Active master is the Standby Master. When performing Active-Standby alternation, the user should press the SWAP button of Active Master and remove the board, or just remove the Active Master directly, the Standby Master will then become Active Master. After Active-Standby alternation, the configuration of the switch will revert to the configuration saved in "startup-config".

6.4 WEB MANAGEMENT

Click the Device management and open the Device Management configuration table.Users can proceed to manage switch modules and display module information and so on.

6.4.1 Reset specific module

Click "Device management", "Reset specific module", select a module number and click "Apply", then that module will be hot-swapped. This function is equal to the CLI command showing in 6.2.1. Click the Reset button to confirm the selection of the module number. Note that the Active master module is not hot-swappable.

6.4.2 Show slot

Click "Device management", "Show slot". An information column will display the current switch's module information. This function is equal to CLI command 6.2.2.1.1.

```
Information display

--------------------Slot : 1--------------------
Inserted:                 YES
Module type:               EM4704BD-M12GX-SFP
Work mode:                 ACTIVE MASTER
Work state:               RUNNING
Software package version:    2.3.9.0
Local software version:      1.2.18.0
Hardware version:           1.1
Bootrom version:           1.5.6
Serial number:             1234567890
Manufacture date:           2005/05/23
Temperature:               36.8750

--------------------Slot : 2--------------------
Inserted:                 NO
Module type:               UNKNOWN
Work mode:                 UNKNOWN
Work state:               NONE
Local software version:
Hardware version:
Bootrom version:
Serial number:
Manufacture date:
Temperature:                0.0000

--------------------Slot : 3--------------------
Inserted:                 NO
Module type:               UNKNOWN
Work mode:                 UNKNOWN
Work state:               NONE
Local software version:
Hardware version:
Bootrom version:
Serial number:
Manufacture date:
Temperature:                0.0000

--------------------Slot : 4--------------------
Inserted:                 NO
Module type:               UNKNOWN
Work mode:                 UNKNOWN
Work state:               NONE
Local software version:
Hardware version:
Bootrom version:
Serial number:
Manufacture date:
Temperature:                0.0000
```

6.4.3 Show fan

Click “Device management”, “Show power”. The information column displayed on the right will show the current power status and display even if the power is plugged in or not. This function is equal to CLI command 6.2.2.1.3.

```
Information display
----------fan information----------
fan board Inserted: YES
```

6.4.4 Show power

Click “Device management”, “Show module” in slot one. The management page will display the

front panel drawing of the switch module and you can see if the physical ports on the module are currently linked up or not. Select to display a certain slot module. The management page will display the front panel drawing of the specified slot module.

6.4.5 Show module in slot

Click “Device management”, “Show module” in slot one. The management page will display the front panel drawing of the switch module one and you can see if the physical ports on the module is linked up or not currently. Select to display slot 2 module, slot 3 module and slot 4. The management page will display the front panel drawing of the specified slot module.

Chapter 7 Port Configuration

7.1 Introduction to Port

ES4704BD comes with line cards and master control boards. Line cards provide various network ports. The master control boards provide no network ports, only Console interface and network management port. The Console interface and network management port are used for out-of-band management of the switch. This chapter focuses on network ports and the network management port.

Network ports are provided by the line cards. The port numbers are marked on the panels of all the line cards for the ES4704BD.To distinguish between ports in different line cards, the port number (in the sense of software) provided by the ES4704BD system is "ethernet X/Y", where X stands for the slot number for the card and Y stands for the number marked in the card panel. For instance, a EM4700BD-12GX-SFP line card is inserted to slot 1, then port 3 of this card corresponds to "ethernet 1/3". If the user needs to configure some network ports, he/she can use the "**interface ethernet <*interface-list*>**" command to enter the appropriate Ethernet port configuration mode, where **<*interface-list*>** stands for one or more ports. If **<*interface-list*>** contains multiple ports, special characters such as ";" or "-" can be used to separate ports, ";" is used for discrete port numbers and "-" is used for consecutive port numbers. Suppose an operation should be performed on ports 2, 3, 4, 5 of the card in slot 1 and ports 8, 9, 10 on the card in slot 3, the command would look like: **interface ethernet 1/2-5;3/8-10.** Port speed, duplex mode and traffic control can be configured under Ethernet Port Mode causing the performance of the corresponding network ports to change accordingly.

The Network management port is located above the Console interface on the master control boards, marked as "Ethernet", the software configuration name for this port is "**Ethernet0**". The user can use the command "**interface Ethernet 0**" to access the network port configuration mode. The user can use programs such as Telnet, Web management and FTP to manage the switch through a Ethernet cable connected to the network management port. The network management port can neither perform data forwarding like the network interfaces, nor use Layer 2 protocols (like RSTP) and Layer 3 routing protocols, nor identify the cable type automatically (such as crossover cables that are required to directly connect to a PC). The network management port supports connection speeds of 10/100 Mbps, it can have an IP address configured in addition to properties such as speed and duplex mode. If the switch has 2 master control cards and both are operating normally, only the Ethernet port in the Active Master can be used as the network management port. When Active-Standby occurs, the network management port will change accordingly.

7.2 Port Configuration

7.2.1 Network Port Configuration

7.2.1.1 Network Port Configuration Task Sequence

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   （1） Configure combo mode for combo ports
   （2） Enable/Disable ports
   （3） Configure port names
   （4） Configure port cable types
   （5） Configure port speed and duplex mode
   （6） Configure bandwidth control
   （7） Configure traffic control
   （8） Enable/Disable port loopback function
   （9） Configure broadcast storm control function for the switch

1. Enter the Ethernet port configuration mode

Command	Explanation
Interface Mode	
interface ethernet <*interface-list*>	Enters the network port configuration mode.

2. Configure the properties for the Ethernet ports

Command	Explanation
Interface Mode	
combo-forced-mode { copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto } **no combo-forced-mode**	Sets the combo port mode (combo ports only); the "**no combo-forced-mode**" command restores the default combo mode for combo ports, i.e., fiber ports first.
shutdown **no shutdown**	Enables/Disables specified ports
name <*string*> **no name**	Names or cancels the name of specified ports
mdi { auto | across | normal } **no mdi**	Sets the cable type for the specified port (This command is not supported on the ES4704BD line card ports of 1000MB and above)

speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }	Sets port speed and duplex mode of 100/1000Base-TX ports. The "no" format of this command restores the default setting, i.e., negotiates speed and duplex mode automatically.
negotiation {on|off}	Enables/Disables the auto-negotiation function of 1000Base-T ports.
bandwidth control <*bandwidth*> [both | receive | transmit] **no bandwidth control**	Sets or cancels the bandwidth used for incoming/outgoing traffic for specified ports
flow control **no flow control**	Enables/Disables traffic control function for specified ports
loopback **no loopback**	Enables/Disables loopback test function for specified ports
rate-suppression {dlf | broadcast | multicast} <packets>	Enables the storm control function for broadcasts, multicasts and unicasts with unknown destinations (short for broadcast), and sets the allowed broadcast packet number; the "no" format of this command disables the broadcast storm control function.

7.2.1.2 Ethernet Port Configuration Commands

7.2.1.2.1 bandwidth

Command: bandwidth control <*bandwidth*> [both | receive | transmit]

no bandwidth control

Function: Enables the bandwidth control function for the port: the **"no bandwidth control"** command disables the bandwidth control function for the port.

Parameters: <***bandwidth***> is the bandwidth limit in Mbps, the valid value ranges from 1 to 10000 Mbps; **both** indicates bandwidth control in both incoming and outgoing traffic; **receive** means bandwidth control applies to incoming traffic from outside the switch; **transmit** means bandwidth control applies to outgoing traffic to outside the switch.

Command mode: Interface Mode

Default: Port bandwidth control is disabled by default.

Usage Guide: When bandwidth control is enable for a port, and bandwidth limit is set, then the maximum bandwidth will be limited and no longer be 10/100/1000M line speed. If **[both | receive | transmit]** keyword is not specified, it will default to **both**.

Note: The bandwidth limit set must not exceed the maximum physical connection speed possible of

the port. For example, a bandwidth limit of 101 M (or more) cannot be set for a 10/100M Ethernet port. But for a 10/100/1000M port working under 100M, a bandwidth limit of 101M (or more) is permitted.

Example: setting the bandwidth limit of ports 1 – 8 of slot 3's card to 40M.

Switch(Config)#interface ethernet 3/1-8

Switch(Config-Port-Range)#bandwidth control 40 both

7.2.1.2.2 combo-forced-mode

Command: combo-forced-mode {copper-forced | copper-preferred-auto | sfp-forced | sfp-preferred-auto }

no combo-forced-mode

Function: Sets to combo port mode (combo ports only); the "**no combo-forced-mode**" command restores to default combo mode for combo ports, i.e., fiber ports first.

Parameters: copper-forced forces use of copper cable ports; **copper-preferred-auto** for copper cable port first; **sfp-forced** for fiber cable forces to use fiber cable port; **sfp-preferred-auto** for fiber cable port first.

Command mode: Interface Mode

Default: The default setting for combo mode of combo ports is fiber cable port first.

Usage Guide: The combo mode of combo ports and the port connection condition determines the active port of the combo ports. A combo port consist of one fiber port and a copper cable port. It should be noted that the speed-duplex command applies to the copper cable port while the negotiation command applies to the fiber cable port, they should not conflict. For combo ports, only one, a fiber cable port or a copper cable port, can be active at a time, and only this port can send and receive data normally.

For the determination of the active port in a combo port, see the table below. The headline row in the table indicates the combo mode of the combo port, while the first column indicates the connection conditions of the combo port, in which "connected" refers to a good connection of fiber cable port or copper cable port to the other devices.

	Copper forced	**Copper preferred**	**SFP forced**	**SFP preferred**
Fiber connected, copper not connected	Copper cable port	Fiber cable port	Fiber cable port	Fiber cable port
Copper connected, fiber not connected	Copper cable port	Copper cable port	Fiber cable port	Copper cable port
Both fiber and copper are connected	Copper cable port	Copper cable port	Fiber cable port	Fiber cable port

Neither fiber nor copper are connected	Copper cable port	Fiber cable port	Fiber cable port	Fiber cable port

Note:

- Combo port is a conception involving the physical layer and the LLC sublayer of the datalink layer. The status of a combo port will not affect any operation in the MAC sublayer of the datalink layer and upper layers. If the bandwidth limit for a combo port is 1Mbps, then this 1Mbps applies to the active port of this combo port, regardless of the port type being copper or fiber.
- If a combo port connects to another combo port, it is recommended for both parties to use copper-forced or fiber-forced mode.
- Run "show interface" under Admin Mode to check for the active port of a combo port The following result indicates if the active port for a combo port is the fiber cable port or copper cable port: Hardware is Gigabit-combo, active is fiber (copper).

Example: setting ports 1/25 -28 to fiber-forced

Switch(Config)#interface ethernet 1/25-28

Switch(Config-Port-Range)#combo-forced-mode sfp-forced

7.2.1.2.3 flow control

Command: flow control

no flow control

Function: Enables the flow control function for the port: the "**no flow control"** command disables the flow control function for the port**.**

Command mode: Interface Mode

Default: Port flow control is disabled by default.

Usage Guide: After the flow control function is enabled, the port will notify the sending device to slow down the sending speed to prevent packet loss when traffic received exceeds the capacity of port cache. ES4704BD's ports support IEEE802.3X flow control; the ports work in half-duplex mode, supporting back-pressure flow control. If flow control results in serious HOL, the switch will automatically start HOL control (discarding some packets in the COS queue that may result in HOL) to prevent drastic degradation of network performance.

Note: Port flow control function is NOT recommended unless the users need a slow speed, low performance network with low packet loss. Flow control will not work between different cards in the switch. When enable the port flow control function, speed and duplex mode of both ends should be the same.

Example: Enabling the flow control function in ports 1/1-8.

Switch(Config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#flow control

7.2.1.2.4 interface ethernet

Command: interface ethernet <*interface-list*>

Function: Enters Ethernet Interface Mode from Global Mode.

Parameters: <*interface-list*> stands for port number.

Command mode: Global Mode

Usage Guide: Run the *exit* command to exit the Ethernet Interface Mode to Global Mode.

Example: Entering the Ethernet Interface Mode for ports 1/1, 2/4-5, 3/8.

Switch(Config)#interface ethernet 1/1;2/4-5;3/8

Switch(Config-Port-Range)#

7.2.1.2.5 loopback

Command: loopback

no loopback

Function: Enables the loopback test function in an Ethernet port; the "**no loopback**" command disables the loopback test on an Ethernet port.

Command mode: Interface Mode

Default: Loopback test is disabled in Ethernet port by default.

Usage Guide: Loopback test can be used to verify the Ethernet ports are working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at the very same port.

Example: Enabling loopback test in Ethernet ports 1/1 – 8

Switch(Config)#interface ethernet 1/1-8

Switch(Config-Port-Range)#loopback

7.2.1.2.6 mdi

Command: mdi { auto | across | normal }

no mdi

Function: Sets the cable types supported by the Ethernet port; the "**no mdi**" command sets the cable type to auto-identification. This command is not supported on ES4704BD line card ports of 1000Mbps or more, these ports have auto-identification set for cable types.

Parameters: auto indicates auto identification of cable types; **across** indicates crossover cable support only; **normal** indicates straight-through cable support only.

Command mode: Interface Mode

Default: Port cable type is set to auto-identification by default.

Usage Guide: Auto-identification is recommended. Generally, straight-through cable is used for switch-PC connection and crossover cable is used for switch-switch connection.

Example: Setting the cable type support of Ethernet ports 3/5 – 8 to straight-through cable only.

Switch(Config)#interface ethernet 3/5-8
Switch(Config-Port-Range)#mdi normal

7.2.1.2.7 name

Command: name <*string*>

no name

Function: Sets a name for the specified port; the "**no name**" command cancels the setting.

Parameters: <*string*> is a string, up to 32 characters are allowed.

Command mode: Interface Mode

Default: No name is set by default.

Usage Guide: This command facilitates the management of the switch. The user can name the ports according to their usage, for example, ports 1/1-2 are used by the financial department, and so can be named "financial"; port 2/9 is used by the engineering department, and can be named "engineering"; port 3/12 connects to the server, and can be named "Servers". Thus, the usage of the ports are obvious.

Example: Naming ports 1/1-2 as "financial"

Switch(Config)#interface ethernet 1/1-2
Switch(Config-Port-Range)#name financial

7.2.1.2.8 negotiation

Command: negotiation {on|off}

Function: Enables/Disables the auto-negotiation function of a 1000Base-T port.

Parameters: on to enable auto-negotiation; **off** to disable auto-negotiation.

Command mode: Port configuration Mode

Default: Auto-negotiation is enabled by default.

Usage Guide: This command applies to 1000Base-T interface only. The **negotiation** command is not available for 1000Base-FX or 100Base-FX interface. . For combo port, this command applies to the 1000Base-TX port only and has no effect on 1000Base-TX port. To change the negotiation mode, speed and duplex mode of 1000Base-TX port, use **speed-duplex** command instead.

Example: Port 1 of Switch 1 is connected to port 1 of Switch 2, the following will disable the negotiation for both ports.

Switch1(Config)#interface e1/1
Switch1(Config-Ethernet1/1)#negotiation off
Switch2(Config)#interface e1/1
Switch2(Config-Ethernet1/1)#negotiation off

7.2.1.2.9 rate-suppression

Command: rate-suppression {dlf | broadcast | multicast} <packets>

no rate-suppression {dlf | broadcast | multicast}

Function: Sets the traffic limit for broadcasts, multicasts and unknown destination unicasts on all ports in the switch; the "**no rate-suppression**" command disables this traffic throttle function on all ports in the switch, i.e., enables broadcasts, multicasts and unknown destination unicasts to pass through the switch at line speed.

Parameters: use **dlf** to limit unicast traffic for unknown destination; **multicast** to limit multicast traffic; **broadcast** to limit broadcast traffic. **<*packets*>** stands for the number of packets allowed to pass through per second for non-10Gb ports. For 10 Gb ports, the number of packets allowed to pass through multiplies 1,040. The valid range for both port types is 1 to 262,143.

Command mode: Interface Mode

Default: no limit is set by default. So, broadcasts, multicasts and unknown destination unicasts are allowed to pass at line speed.

Usage Guide: All ports in the switch belong to a same broadcast domain if no VLAN has been set. The switch will send the abovementioned three traffics to all ports in the broadcast domain, which may result in broadcast storm and so may greatly degrade the switch performance. Enabling Broadcast Storm Control can better protect the switch from broadcast storm. Note the difference of this command in 10Gb ports and other ports. If the allowed traffic is set to 3, this means allow 3,120 packets per second and discard the rest for 10Gb ports. However, the same setting for non-10Gb ports means to allow 3 broadcast packets per second and discard the rest.

Example: Setting ports 8 – 10 (1000Mbps) of slot 2 to allow 3 broadcast packets per second.

Switch(Config)#interface ethernet 2/8-10

Switch(Config-Port-Range)#rate-suppression broadcast 3

7.2.1.2.10 shutdown

Command: shutdown

no shutdown

Function: Shuts down the specified Ethernet port; the "**no shutdown**" command opens the port.

Command mode: Interface Mode

Default: Ethernet port is open by default.

Usage Guide: When Ethernet port is shut down, no data frames are sent in the port, and the port status displayed when the user types the "**show interface**" command is "down".

Example: Opening ports 1/1-8.

Switch(Config)#interface ethernet1/1-8

Switch(Config-Port-Range)#no shutdown

7.2.1.2.11 speed-duplex

Command: speed-duplex {auto | force10-half | force10-full | force100-half | force100-full | { {force1g-half | force1g-full} [nonegotiate [master | slave]] } }

no speed-duplex

Function: Sets the speed and duplex mode for 1000Base-TX or 100Base-TX ports; the "**no speed-duplex**" command restores the default speed and duplex mode setting, i.e., auto speed negotiation and duplex.

Parameters: auto for auto speed negotiation; **force10-half** for forced 10Mbps at half-duplex; **force10-full** for forced 10Mbps at full-duplex mode; **force100-half** for forced 100Mbps at half-duplex mode; **force100-full** for forced 100Mbps at full-duplex mode; **force1g-half** for forced 1000Mbps at half-duplex mode; **force1g-full** for forced 1000Mbps at full-duplex mode; **nonegotiate** for disable auto-negotiation for 1000 Mb port; **master** to force the 1000Mb port to be **master** mode; **slave** to force the 1000Mb port to be **slave** mode.

Command mode: Port configuration Mode

Default: Auto-negotiation for speed and duplex mode is set by default.

Usage Guide: This command applies to 1000Base-TX or 100Base-TX ports only. **speed-duple**x command is not available for 1000Base-X port. For combo port, this command applies to the 1000Base-TX port only and has no effect on 1000Base-X port. To change the negotiation mode of 1000Base-X port, use **negotiation** command instead.

When configuring port speed and duplex mode, the speed and duplex mode must be the same as the setting of the remote end, i.e., if the remote device is set to auto-negotiation, then auto-negotiation should be set at the local port. If the remote end is in forced mode, the same should be set in the local end.

1000Gb ports are by default **master** when configuring **nonegotiate** mode. If one end is set to **master** mode, the other end must be set to **slave** mode. **force1g-half** Is not supported yet.

Example: Port 1 of Switch 1 is connected to port 1 of Switch2, the following will set both ports in forced 100Mbps at half-duplex mode.

Switch1(Config)#interface e1/1

Switch1(Config-Ethernet1/1)#speed-duplex force100-half

Switch2(Config)#interface e1/1

Switch2(Config-Ethernet1/1)#speed-duplex force100-half

7.2.2 VLAN Interface Configuration

7.2.2.1 VLAN Interface Configuration Task Sequence

1. Enter VLAN Mode
2. Configure the IP address for VLAN interface and enable VLAN interface.

1. Enter VLAN Mode

Command	Explanation
Global Mode	
interface vlan <*vlan-id*> **no interface vlan <*vlan-id*>**	Enters VLAN Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes specified VLAN interface. .

2. Configure the IP address for VLAN interface and enables VLAN interface.

Command	Explanation
VLAN Mode	
ip address <*ip-address*> <*mask*> [secondary] **no ip address [<*ip-address*> <*mask*>]**	Configures the VLAN interface IP address; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the VLAN interface IP address.
VLAN Mode	
Shutdown **no shutdown**	Enables/Disables VLAN interface

7.2.2.2 VLAN Interface Configuration Commands

7.2.2.2.1 interface vlan

Command: interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Enters VLAN Interface Mode; the "**no interface vlan <*vlan-id*>**" command deletes existing VLAN interface. .

Parameters: <*vlan-id*> is the VLAN ID for the establish VLAN, the valid range is 1 to 4094.

Command mode: Global Mode

Usage Guide: Before setting a VLAN interface, the existence of the VLAN must be verified. Run the *exit* command to exit the VLAN Mode to Global Mode.

Example: Entering into the VLAN Interface Mode for VLAN1.

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#

7.2.2.2.2 ip address

Command: ip address <*ip-address*> <*mask*> [secondary]

no ip address [<*ip-address*> <*mask*>] [secondary]

Function: Sets the IP address and mask for the switch; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the specified IP address setting.

Parameters: **<*ip-address*>** is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format; **[secondary]** indicates the IP configured is a secondary IP address.

Command mode: VLAN Interface Mode

Default: No IP address is configured by default.

Usage Guide: This command configures the IP address for VLAN interface manually. If the optional parameter secondary is not present, the IP address will be the primary IP of the VLAN interface, otherwise, the IP address configured will be the secondary IP address for the VLAN interface. A VLAN interface can have one primary IP address but multiple secondary IP addresses. Both primary IP address and secondary IP addresses can be used for SNMP/Web/Telnet management. In addition, ES4704BD allows IP addresses to be obtained through BootP/DHCP.

Example: Setting the IP address of VLAN1 interface to 192.168.1.10/24.

Switch(Config-If-Vlan1)#ip address 192.168.1.10 255.255.255.0

7.2.2.2.3 shutdown

Command: shutdown

no shutdown

Function: Shuts down the specified VLAN Interface; the "**no shutdown**" command opens the VLAN interface.

Command mode: VLAN Interface Mode

Default: VLAN Interface is enabled by default.

Usage Guide: When VLAN interface is shutdown, no data frames will be sent by the VLAN interface. If the VLAN interface needs to obtain IP address via BootP/DHCP protocol, it must be enabled.

Example: Enabling VLAN1 interface of the switch.

Switch(Config-If-Vlan1)#no shutdown

7.2.3 Network Management Port Configuration

7.2.3.1 Network Management Port Configuration Task Sequence

1. Enter the network management port configuration mode
2. Configure the properties for the network management ports
   （1） Enable/Disable ports
   （2） Configure port speed
   （3） Configure port duplex mode
   （4） Enable/Disable port loopback function
   （5） Configuring port IP Address

1. Enter the network management port configuration mode

Command	Explanation
Global Mode	
interface ethernet <*num*>	Enters the network management port configuration mode

2. Configure the properties for the network management port

Command	Explanation
Network Management Port Configuration	
shutdown **no shutdown**	Enables/Disables network management port
speed {auto| force10| force100| }	Sets network management port speed
duplex {auto| full| half}	Sets network management port duplex mode
loopback **no loopback**	Enables/Disables loopback test function for network management port
ip address <ip-address> <mask> **no ip address [<ip-address> <mask>]**	Configures or cancels the IP address for network management port.

7.2.3.2 Network Management Port Configuration Commands

7.2.3.2.1 duplex

Command: duplex {auto| full| half }

Function: Sets network management port duplex mode

Parameters: auto for auto-negotiation full-duplex mode; **full** for forced full-duplex mode; **half** for forced half-duplex mode.

Command mode: Network management port configuration Mode

Default: The default duplex mode is set to auto-negotiation.

Usage Guide: According to IEEE 802.3, the auto-negotiation for port speed and duplex are linked. If the duplex setting of the port is auto-negotiation, the port speed will be set to auto-negotiation automatically; if the port duplex mode changes from auto-negotiation to forced full/half-duplex, the port speed will also become forced mode, the forced speed will be the port speed before this command.

It is strongly recommended for the users to set all port speed and duplex mode to auto-negotiation, this can minimize protocol-related connection problems. If forced speed/duplex mode needs to be set, the speed/duplex mode setting of both ends must be verified to be the same.

Example: Setting the network management port to forced full-duplex mode.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#duplex full

7.2.3.2.2 interface ethernet

Command: interface ethernet <*interface-name*>

Function: Enters network management port configuration mode from Global Mode.

Parameters: <*interface-name*> stands for port number, the default value is 0.

Command mode: Global Mode

Usage Guide: Run the *exit* command to exit the network management Interface Mode to Global Mode.

Example: Entering network management interface mode.

Switch(Config)#interface ethernet 0

Switch(Config-Ethernet0)#

7.2.3.2.3 ip address

Command: ip address <*ip-address*> <*mask*>

no ip address [<*ip-address*> <*mask*>]

Function: Sets the IP address and mask for the switch; the "**no ip address [<*ip-address*> <*mask*>]"** command deletes the specified IP address setting.

Parameters: <*ip-address*> is the IP address in decimal format; **<*mask*>** is the subnet mask in decimal format.

Command mode: Network management port configuration Mode

Default: No IP address is configured by default.

Usage Guide: This command configures the IP address for network management port.

Example: Setting the IP address of the network management interface to 192.168.1.10/24.

Switch(Config-Ethernet0)#ip address 192.168.1.10 255.255.255.0

7.2.3.2.4 loopback

Command: loopback

no loopback

Function: Enables the loopback test function for the network management port; the "**no loopback**" command disables the loopback test the on network management port.

Command mode: Network management port configuration Mode

Default: Loopback test is disabled in network management port by default.

Usage Guide: Loopback test can be used to verify the network management port is working normally. After loopback has been enabled, the port will assume a connection established to itself, and all traffic sent from the port will be received at this very port.

Example: Enabling loopback test in the network management port.

Switch(Config)#interface ethernet 0
Switch(Config-Ethernet0)#loopback

7.2.3.2.5 shutdown

Command: shutdown
no shutdown

Function: Shuts down the network management port; the "**no shutdown**" command opens the port.

Command mode: Network management port configuration Mode

Default: Network management port is open by default.

Usage Guide: When network management port is shut down, no data frames are sent in the port, and the port status displayed when the user typed "**show interface**" command is "down".

Example: Enabling the network management interface.

Switch(Config)#interface ethernet 0
Switch(Config-Ethernet0)#no shutdown

7.2.3.2.6 speed

Command: speed {auto| force10| force100}

Function: Sets port speed

Parameters: auto for auto-negotiation of speed; **force10** for forced 10Mbps; **force100** for forced half 100Mbps.

Command mode: Network management port configuration Mode

Default: Auto-negotiation for speed is set by default.

Usage Guide: According to IEEE 802.3, the auto-negotiation for port speed and duplex are linked. If the port speed setting is auto-negotiation, the port duplex mode will also be set to auto-negotiation automatically; if the port speed changes from auto-negotiation to forced, the port duplex mode will also become forced full/half-duplex.

It is strongly recommended for users to set all port speed and duplex mode to auto-negotiation, this can minimize protocol-related connection problems. If forced speed/duplex mode needs to be set, the speed/duplex mode setting of both ends must be verified to be the same.

Example: Setting the network management port to forced 100Mbps.

Switch(Config)#interface ethernet 0
Switch(Config-Ethernet0)#speed force100

7.2.4 Port Mirroring Configuration

7.2.4.1 Introduction to Port Mirroring

Port mirroring refers to the duplication of data frames sent/received on a port to another port. The duplicated port is referred to as mirror source port and the duplicating port is referred to as

mirror destination port. A protocol analyzer (such as Sniffer) or RMON monitoring instrument is often attached to the mirror destination port to monitor and manage the network and diagnostic.

ES4704BD support one mirror destination port only. The number of mirror source ports are not limited, one or more may be used. Multiple source ports can be within the same VLAN or across several VLANs. The destination port and source port(s) can be located in different VLANs.

7.2.4.2 Port Mirroring Configuration Task Sequence

1. Specify mirror source port
2. Specify mirror destination port

1. Specify mirror source port

Command	Explanation
Global Mode	
monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]} {rx| tx| both} **no monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]}**	Specifies mirror source port; the " **no monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]}**" command deletes mirror source port.

2. Specify mirror destination port

Command	Explanation
Global Mode	
monitor session <*session*> destination interface <*interface-number*> **no monitor session <*session*> destination interface <*interface-number*>**	Specifies the mirror destination port; the "**no monitor session <*session*> destination interface <*interface-number*>**" command deletes mirror destination port.

7.2.4.3 Port Mirroring Configuration

7.2.4.3.1 monitor session source interface

Command: monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]} {rx| tx| both}

no monitor session <*session*> source {interface <*interface-list*> | cpu [slot <*slotnum*>]}

Function: Specifies the mirror source port; the "**no monitor session <*session*> source interface**

<***interface-list***>" command deletes mirror source port.

Parameters: <***session***> stands for mirror session value, only 1 may be used at present; <***interface-list***> stands for mirror source port list, special characters like "-" and ";" are supported; **cpu slot** <***slotnum***> stands for use the CPU of the card in the specified slot as mirror source, to mirroring traffic sent/received by the CPU (for debug); **rx** stands for traffic received by the source port; **tx** stands for traffic sent by the source port; **both** stands for traffic sent and received by the source port.

Command mode: Global Mode

Usage Guide: This command sets the source port for mirroring. ES4704BD does not have any limit on the number mirror source port(s). The sent and/or received traffic by the source port can be mirrored. If **[rx|tx|both]** keyword is not specified, it will default to **both**. When multiple ports are mirrored, their mirrored traffic direction can be different, but should be configured separately.

Example: Setting the mirror source port to be the outgoing traffic of ports 1/1-4 and incoming traffic of port 3/5.

Switch(Config)#monitor session 1 source interface ethernet 1/1-4 tx

Switch(Config)#monitor session 1 source interface ethernet 3/5 rx

7.2.4.3.2 monitor session destination interface

Command: monitor session <*session*> destination interface <*interface-number*>

no monitor session <*session*> destination interface <*interface-number*>

Function: Specifies mirror destination port; the "**no monitor session <*session*> destination interface <*interface-number*>**" command deletes mirror destination port.

Parameters: <***session***> set the mirror session value, only 1 may be used at present; <***interface-number***> sets the mirror destination port.

Default: N/A.

Command mode: Global Mode

Usage Guide: Only one mirror destination port is supported by ES4704BD. It should be noted that the mirror destination port can not be a member of a trunk group, and it is desirable for its port throughput to be greater than the total sum throughput of all the mirror source ports.

Example: Setting port 4/7 as mirror destination port.

Switch(Config)#monitor session 1 destination interface ethernet 4/7

7.2.4.4 Port Mirroring Examples

See "Port Configuration Examples".

7.2.4.5 Device Mirroring Troubleshooting Help

7.2.4.5.1 Monitor and Debug Commands

7.2.4.5.1.1 show monitor

Command: show monitor

Function: Displays information about mirror source/destination ports.

Command mode: Admin Mode

Usage Guide: This command displays the mirror source port(s) and destination port currently configured.

Example:

Switch#show monitor

7.2.4.5.2 Device Mirroring Troubleshooting Help

If a problems occurs configuring port mirroring, please check the following first for causes:

- ☞ Whether the mirror destination port is a member of a trunk group or not, if yes, modify the trunk group.
- ☞ If the throughput of mirror destination port is smaller than the total throughput of mirror source port(s), the destination port will not be able to duplicate all source port traffic; please decrease the number of source ports, duplicate traffic for one direction only or choose a port with greater throughput as the destination port.

7.3 Port Configuration Example

Fig 7-1 Port Configuration Example

No VLAN has been configured in the switches, default VLAN1 is used.

Switch	Port	Property
SW1	2/7	Ingress bandwidth limit: 150 M
SW2	1/8	Mirror source port
	3/9	100Mbps full, mirror source port
	4/12	1000Mbps full, mirror destination port
SW3	4/10	100Mbps full

The configurations are listed below:

SW1：

Switch1(Config)#interface ethernet 2/7

Switch1(Config-Ethernet2/7)#bandwidth control 150 both

SW2：

Switch2(Config)#interface ethernet 3/9

Switch2(Config- Ethernet3/9)# speed-duplex force100-full

Switch2(Config- Ethernet3/9)#exit

Switch2(Config)#interface ethernet 4/12

Switch2(Config-Ethernet4/12)# speed-duplex force1000-full

Switch2(Config-Ethernet4/12)#exit

Switch2(Config)#monitor session 1 source interface ethernet 1/8;3/9

Switch2(Config)#monitor session 1 destination interface ethernet 4/12

SW3：

Switch3(Config)#interface ethernet 4/10

Switch3(Config-Ethernet4/10)# speed-duplex force100-full

Switch3(Config-Ethernet4/10)#exit

7.4 Port Troubleshooting Help

7.4.1 Monitor and Debug Commands

7.4.1.1 clear counters

Command: clear counters [{ethernet <*interface-list*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]

Function: Clears the statistics of the specified port.

Parameters: <***interface-list***> stands for the Ethernet port number; < ***vlan-id*** > stands for the VLAN interface number; <***port-channel-number***> for trunk interface number; <***interface-name***> for interface name, such as port-channel 1.

Command mode: Admin Mode

Default: Port statistics are not cleared by default.

Usage Guide: If no port is specified, then statistics of all ports will be cleared.

Example: Clearing the statistics for Ethernet port 1/1.

Switch#clear counters ethernet 1/1

7.4.1.2 show interface

Command: show interface [{ethernet <*interface-number*> | vlan <*vlan-id*> | port-channel <*port-channel-number*> | <*interface-name*>}]

Function: Displays information about specified port.

Parameters: <***interface-number***> stands for the Ethernet port number; < ***vlan-id*** > stands for the VLAN interface number; <***port-channel-number***> for trunk interface number; <***interface-name***> for interface name, such as port-channel 1.

Command mode: Admin Mode

Default: No port information is displayed by default.

Usage Guide: For Ethernet ports, this command displays information about port speed, duplex mode, traffic control on/off, broadcast storm control and statistics for packets sent/received; for

VLAN interfaces, this command displays MAC address, IP address and statistics for packets sent/received; for trunk ports, this command displays port speed, duplex mode, traffic control on/off, broadcast storm control and statistics for packets sent/received. Usage Guide: If no ports are specified, then information for all ports will be displayed.

Example: Displaying information about port 4/1.

Switch#show interface ethernet 4/1

7.4.2 Port Troubleshooting Help

Here are some situations that frequently occurs in port configuration and the advised solutions:

- ☞ Two connected fiber interfaces won't link up if one interface is set to auto-negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.
- ☞ The following combinations are not recommended: enabling traffic control as well as setting multicast limiting for the same port; setting broadcast, multicast and unknown destination unicast control as well as port bandwidth limiting for the same port. If such combinations are set, the port throughput may fall below the expected performance.

7.5 WEB MANAGEMENT

Click "Port configuration" to open the port configuration management table. Users can proceed to do port management, setup port speed, duplexes and so on.

7.5.1 Ethernet port configuration

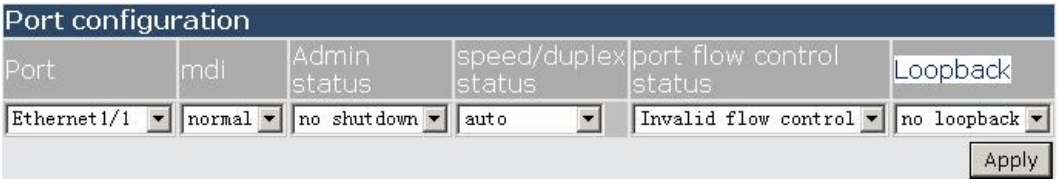
Click "Port configuration", "Ethernet port configuration" to open the Ethernet port configuration management table to configure Ethernet port duplex, speed, bandwidth control and so on.

7.5.1.1 Physical port configuration

Click "port configuration", "Ethernet port configuration", "Physical port configuration" to configure the following information:

- Port: Specifies the configuration port
- MDI: Sets up the connection type of the Ethernet port. Auto means to auto-negotiate connection type; across means the port supporting cross-over cable only; normal means the port supporting straight-through cable only. This function is equal to CLI command 7.2.1.2.6.
- Admin Status: Enables/Disables port. Equals to CLI command 7.2.1.2.9
- speed/duplex status: Sets up Ethernet sport speed and duplex including, auto-negotiation, 10Mbps Half, 10Mbps Full, 100Mbps Half, 100Mbps Full, 1000Mbps Half, 1000Mbps Full. Equals to CLI command 7.2.1.2. and 7.2.1.2.10
- Port flow control status: Sets up port flow control including disabled flow control and enabled flow control. Equals to CLI command 7.2.1.2.3
- Loopback: Sets up Ethernet port to enable loopback testing function. Equals to CLI command 7.2.1.2.5

Example: Assign port to be Ethernet 1/1 and set up MDI as normal; Admin control status as no shutdown, speed/duplex as auto, port flow control status as disabled flow control and Loopback as no loopback. Then click Apply button and these set up items will be applied to port 1/1.



Port list table displays the related information of the switch physical ports.

Port list

Port	mdi	Status	Speed	Mode	Flow control	loopback
Ethernet1/1	auto	UP	auto	auto	Non flow control state	no loopback
Ethernet1/2	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/3	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/4	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/5	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/6	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/7	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/8	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/9	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/10	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/11	auto	DOWN	auto	auto	Non flow control state	no loopback
Ethernet1/12	auto	DOWN	auto	auto	Non flow control state	no loopback

7.5.1.2 Bandwidth control

Click port configuration, Ethernet port configuration, Bandwidth control and proceed to do port bandwidth control. Equals to CLI command 7.2.1.2.1

- Port: Specifies configuration port
- Bandwidth control level: port bandwidth control. The unit is Mbps and the value range is 1~10000Mbps
- Control type: Ingress means to control port bandwidth when receiving data packet sent from outside the switch. Egress means to control port bandwidth when sending data packets to outside of the switch. Ingress and Egress means to control port bandwidth when both receiving and sending.

Example: Choose Port to be Ethernet 2/1, set up Bandwidth control level as 100Mb, Control type as Ingress, then click Apply button. So the port 1/1 will execute bandwidth control and receiving data packet with 100M.

Port list table displays the port bandwidth control information of the switch:

Port list		
Port Num	Ingress bandwidth threshold(Mb)	Outgress bandwidth threshold(Mb)
Ethernet2/1	100	Have not set
Ethernet2/2	Have not set	Have not set
Ethernet2/3	Have not set	Have not set
Ethernet2/4	Have not set	Have not set
Ethernet2/5	Have not set	Have not set
Ethernet2/6	Have not set	Have not set
Ethernet2/7	Have not set	Have not set
Ethernet2/8	Have not set	Have not set
Ethernet2/9	Have not set	Have not set
Ethernet2/10	Have not set	Have not set
Ethernet2/11	Have not set	Have not set
Ethernet2/12	Have not set	Have not set

7.5.2 Vlan interface configuration

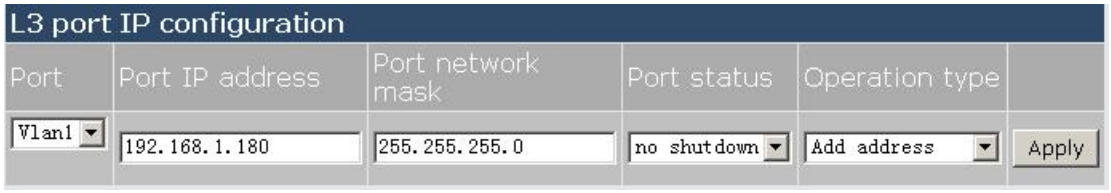
Click Port configuration, vlan interface configuration to open the VLAN port configuration management list to allocate IP address and mask on L3 port and so on.

7.5.2.1 Allocate IP address for L3 port

Click “Port configuration”, “vlan interface configuration”, Allocate IP address for L3 port to allocate IP address for L3 port. Equals to CLI command 7.2.2.2.2. This setup contains the following characteristics:

- Port: L3 port
- Port IP address: IP address for L3 port
- Port network mask
- Port status
- Operation type: add/delete address

Example: Assign Port as Vlan1, port IP address as 192.168.1.180, Port network mask as 255.255.255.0, Port status as no shutdown, Operation type selection as Add address then click Apply button and this set up will be applied to the switch.

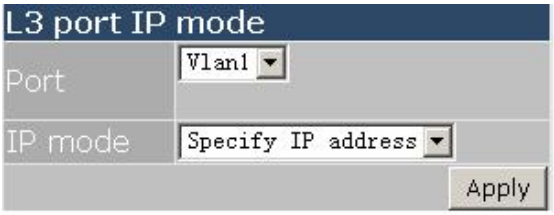


7.5.2.2 L3 port IP addr mode configuration

Click “Port configuration”, “vlan interface configuration”, “L3 port IP addr mode configuration” to set up L3 port IP address mode configuration.

- Port: L3 port
- IP mode: Specifies the Ip address, meaning users need to set up L3 IP address manually. Bootp-client means to gain an IP address and gateway address through BootP. Equals to CLI command 5.3.2.2. dhcp-client means to gain IP address and gateway address through DHCP. Equals to CLI command 5.3.2.3

Example: Specify L3 port as Vlan 1 and the IP mode as Specify IP address. Click the apply button and this setup will be applied to the switch.



7.5.3 Port mirroring configuration

Click “Port configuration”, “Port mirroring configuration” to enter port mirroring configuration management table to do port mirroring configurations.

7.5.3.1 Mirror configuration

Click Port configuration, Port mirroring configuration, Mirror configuration to configure port mirroring function including configuring mirroring source port and mirroring destination port functions.

Configure mirroring source port equals to CLI command 7.2.3.3.1:

- Session: Mirror dialog value
- source interface list
- Mirror direction: rx means to mirror the port receiving data packets; tx means to mirror the port sending data packets; both means to mirror both receiving & sending

Example: Select mirror dialog session as one, set up source interface list as Ethernet ports 1/1~4 and the mirroring direction as rx. Click Apply button and this port will be added into the monitor session. Click the Default button to delete this port from the list.

Configure mirroring destination port. Equals to CLI command 7.2.3.3.2.

- Session: Mirroring dialog value
- destination interface
- tag: Setting the vlan tag function means all mirroring packets carry vlan tags; preserve means that if the Ingress mirroring packet, carrying a vlan tag, while Ingress, then Egress mirroring packet will carry vlan tag as well. Otherwise will be not.

Example: Select mirror dialog session as 1 and set up port mirroring list as 1/5, tag as preserve. Click Apply button and this setting will be applied in the switch.

7.5.4 Port debug and maintenance

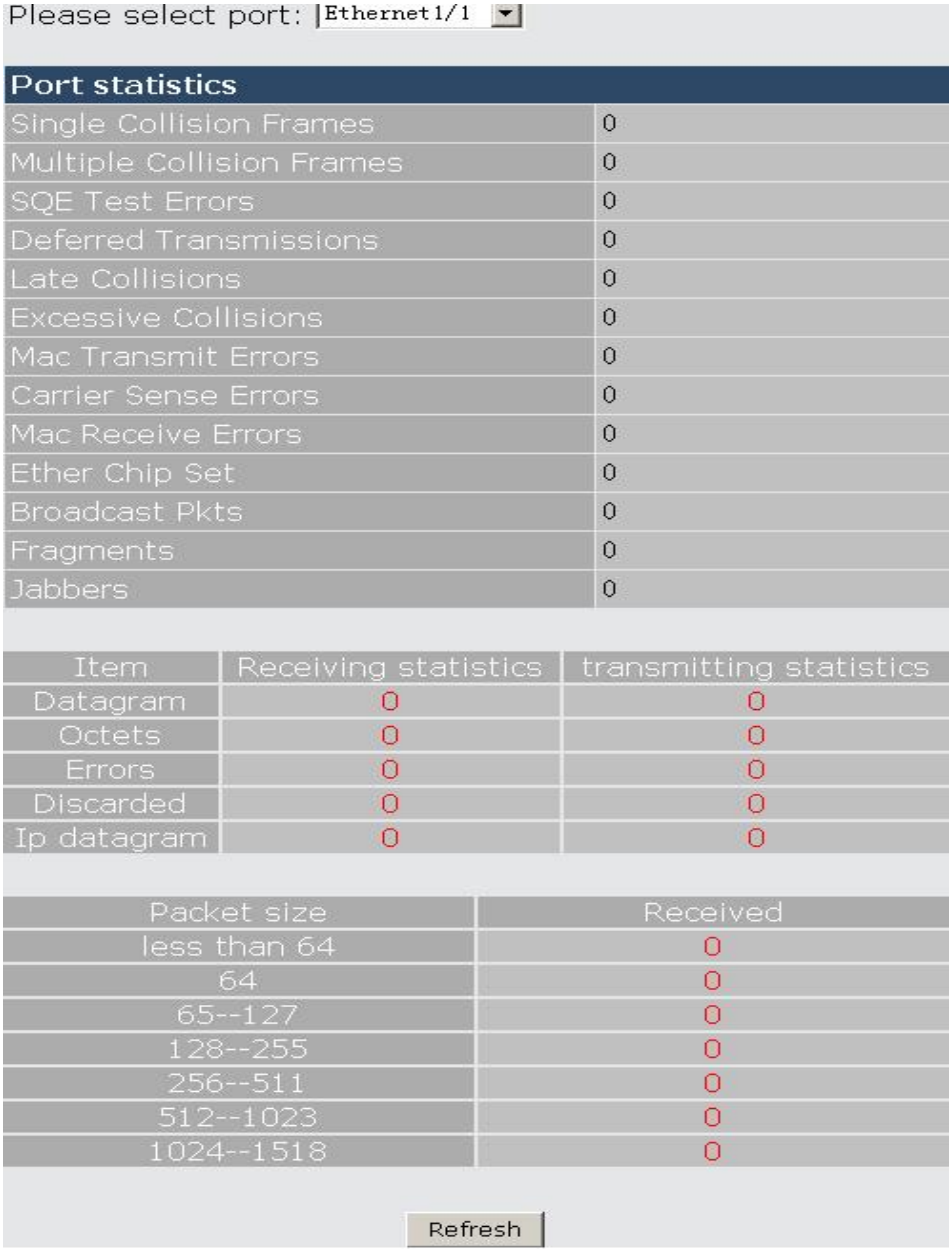
Click Port configuration, Port debug and maintenance and open the Port debug and maintenance

management list to get port information.

7.5.4.1 Show port information

Click “Port configuration”, “Port debug” and “maintenance”, Show port information to check the statistic information of the receiving/sending data packet information of the port. Equals to CLI command 7.4.1.2

Example: Select check Ethernet port 1/1 and click Refresh to see the statistic report of port 1/1



Chapter 8 MAC Table Configuration

8.1 Introduction to MAC Table

MAC table identifies the mapping relationship between destination MAC addresses and switch ports. MAC addresses can be categorized as static MAC addresses and dynamic MAC addresses. Static MAC addresses are manually configured by the user, have the highest priority and are permanently effective (they will not be overwritten by dynamic MAC addresses); dynamic MAC addresses are entries learnt by the switch in data frame forwarding, and are effective for a limited period. When the switch receives a data frame to be forwarded, it stores the source MAC address of the data frame and creates a mapping to the destination port. Then, the MAC table is queried for the destination MAC address, if hit, the data frame is forwarded to the associated port, otherwise, the switch forwards the data frame to its broadcast domain. If a dynamic MAC address is not learnt from the data frames to be forwarded for a long time, the entry will be deleted from the switch's MAC table.

There are two MAC table operations:

1. Obtain a MAC address
2. Forward or filter data frame according to the MAC table

8.1.1 Obtaining MAC Table

The MAC table can be built by static configuration and dynamic learning. Static configuration sets up a mapping between the MAC addresses and the ports, Dynamic learning is the process in which the switch learns the mapping between MAC addresses and ports, and updates the MAC table regularly. In this section, we will focus on the dynamic learning process of MAC table.

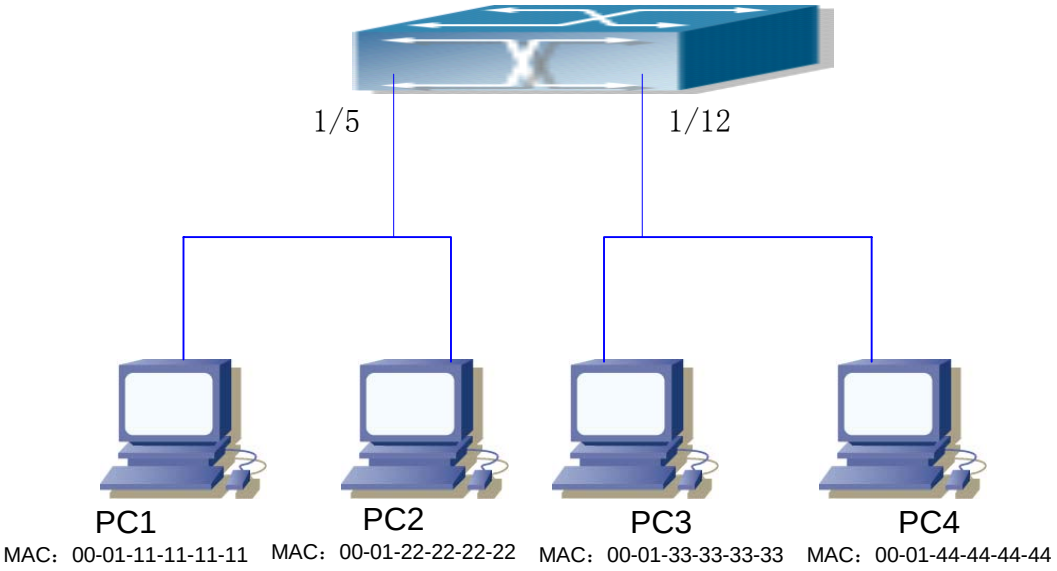


Fig 8-1 MAC Table dynamic learning

The topology of the figure above: 4 PCs connected to ES4704BD, where PC1 and PC2 belong to a same physical segment (same collision domain), the physical segment connects to port 1/5 of ES4704BD; PC3 and PC4 belong to the same physical segment that connects to port 1/12 of ES4704BD.

The initial MAC table contains no entries. Take the communication of PC1 and PC3 as an example, the MAC address learning process is as follows:

1. When PC1 is sending a message to PC3, the switch receives the source MAC address 00-01-11-11-11-11 for this message, the mapping entry of 00-01-11-11-11-11 and port 1/5 is added to the switch MAC table.
2. At the same time, the switch learns the message is destined to 00-01-33-33-33-33, as the MAC table contains only a mapping entry of MAC address 00-01-11-11-11-11 and port 1/5, and no port mapping for 00-01-33-33-33-33 present, the switch broadcasts this message to all the ports in the switch (assuming all ports belong to the default VLAN).
3. PC3 and PC4 on port 1/12 receive the message sent by PC1. PC4 will not reply, as the destination MAC address is 00-01-33-33-33-33 Only PC3 will reply to PC1. When port 1/12 receives the message sent by PC3, a mapping entry for MAC address 00-01-33-33-33-33 and port 1/12 is added to the MAC table.
4. Now the MAC table has two dynamic entries, MAC address 00-01-11-11-11-11, port 1/5 and 00-01-33-33-33-33, port 1/12.
5. After the communication between PC1 and PC3, the switch does not receive any messages sent from PC1 and PC3. And the MAC address mapping entries in the MAC table are deleted after 300 seconds. The 300 seconds here is the default aging time for MAC address entry in ES4704BD. Aging time can be modified in ES4704BD.

8.1.2 Forward or Filter

The switch will forward or filter received data frames according to the MAC table. Take the above figure as an example, assuming ES4704BD has learnt the MAC address of PC1 and PC3, and the user manually configured the mapping relationship for PC2 and PC4 to ports. The MAC table of ES4704BD would be:

MAC Address	Port number	Entry added by
00-01-11-11-11-11	1/5	Dynamic learning
00-01-22-22-22-22	1/5	Static configuration
00-01-33-33-33-33	1/12	Dynamic learning
00-01-44-44-44-44	1/12	Static configuration

1. Forward data according to the MAC table

If PC1 sends a message to PC3, the switch will forward the data received on port 1/5 to port 1/12.

2. Filter data according to the MAC table

If PC1 sends a message to PC2, the switch, on checking the MAC table, will find PC2 and PC1 are in the same physical segment and filter the message (i.e., drop this message).

Three types of frames can be forwarded by the switch:

- ✧ Broadcast frame
- ✧ Multicast frame
- ✧ Unicast frame

The following describes how the switch deals with all the three types of frames:

1. Broadcast frames: The switch can segregate collision domains but not broadcast domains. If no VLAN has been set, all devices connected to the switch are in the same broadcast domain. When the switch receives a broadcast frame, it forwards the frame to all ports. When VLANs are configured in the switch, the MAC table will be adapted accordingly to add VLAN information. In this case, the switch will not forward the received broadcast frames to all ports, but forward the frames to all ports in the same VLAN.
2. Multicast frames: If IGMP Snooping function has not been enabled, multicast frames are processed in the same way as broadcast frames; when IGMP Snooping has been enabled, the switch will only forward the multicast frame to the ports belonging to the very multicast group.
3. Unicast frames: If no VLAN has been configured and the destination MAC addresses are in the switch MAC table, the switch will directly forward the frames to the associated ports; if the destination MAC address in a unicast frame were not found in the MAC table, the switch will broadcast the unicast frame. When VLANs are configured, the switch will forward unicast frames within the same VLAN. If the destination MAC address is found in the MAC table but belongs to different VLANs, the switch can still only broadcast the unicast frame in the VLAN it belongs to.

8.2 MAC Table Configuration

8.2.1 mac-address-table aging-time

Command: mac-address-table aging-time {<*age*>| 0}

no mac-address-table aging-time

Function: Sets the aging time for address mapping entries in the MAC table that have been dynamically learnt; the "**no mac-address-table aging-time**" command restores the aging time to the default time of 300 seconds.

Parameters: < *age*> is the aging time in seconds, the valid range is 10 to 100000; 0 for no aging.

Command mode: Global Mode

Default: The system default aging time is 300 seconds.

Usage Guide: A too short aging time results in many unnecessary broadcasts and causing performance degradation; too long aging time will leave some obsolete entries occupying MAC table space of. For this reason, the user should set a reasonable aging time according to the production conditions.

If the aging time is set to 0, addresses dynamically learned by the switch will not age in time, the addresses learned will be kept in the MAC table permanently.

Example: Setting the aging time for dynamically learned entries in the MAC table to 400 seconds.

Switch(Config)#mac-address-table aging-time 400

8.2.2 mac-address-table static

Command: mac-address-table static address <*mac-addr*> vlan <*vlan-id*> interface <*interface-name*>

no mac-address-table [{static | dynamic} [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>]]

Function: Adds or modifies static address entries, the "**no mac-address-table**" command deletes static address entries and dynamic address entries.

Parameters: static stands for static address entry; **dynamic** for dynamic address entry; **<*mac-addr*>** for MAC address to be added or deleted; **<*interface-name*>** for port name to forward the MAC frame; **<*vlan-id*>** for VLAN number.

Command mode: Global Mode

Default: When configuring a VLAN interface, the system will generate a static address mapping entry for a system inherent MAC address and the VLAN number.

Usage Guide: For special purposes or if the switch can not learn MAC address dynamically, the user can use this command to establish mapping relationships between MAC addresses and ports/VLAN.

"**no mac-address-table**" command will delete and filter all existing dynamic or static MAC address

entries, except system default reserved entries.

Example: Port 1/1 belongs to VLAN200, set a mapping to MAC address 00-03-0f-f0-00-18.

Switch(Config)#mac-address-table static address 00-03-0f-f0-00-18 vlan 200 interface ethernet 1/1

8.2.3 mac-address-table blackhole

Command: mac-address-table blackhole address <*mac-addr*> vlan <*vlan-id* >

no mac-address-table blackhole [address <*mac-addr*>] [vlan <*vlan-id*>]

Function: Adds or modifies filter address entries, the "**no mac-address-table blackhole**" command deletes filter address entries.

Parameters: blackhole stands for a filter entry, filter entries are configured to discard frames of specified MAC addresses, so that traffic can be filtered. Both source addresses and destination addresses can be filtered. **<*mac-addr*>** stands for MAC addresses to be added or deleted, **<*vlan-id*>** for VLAN number.

Command mode: Global Mode

Usage Guide: "**no mac-address-table blackhole**" command will delete all filter MAC address entries in the switch MAC table.

Example: Setting 00-03-0f-f0-00-18 to be a filter MAC address entry for VLAN200.

Switch(Config)#mac-address-table blackhole address 00-03-0f-f0-00-18 vlan 200

8.3 Typical Configuration Examples

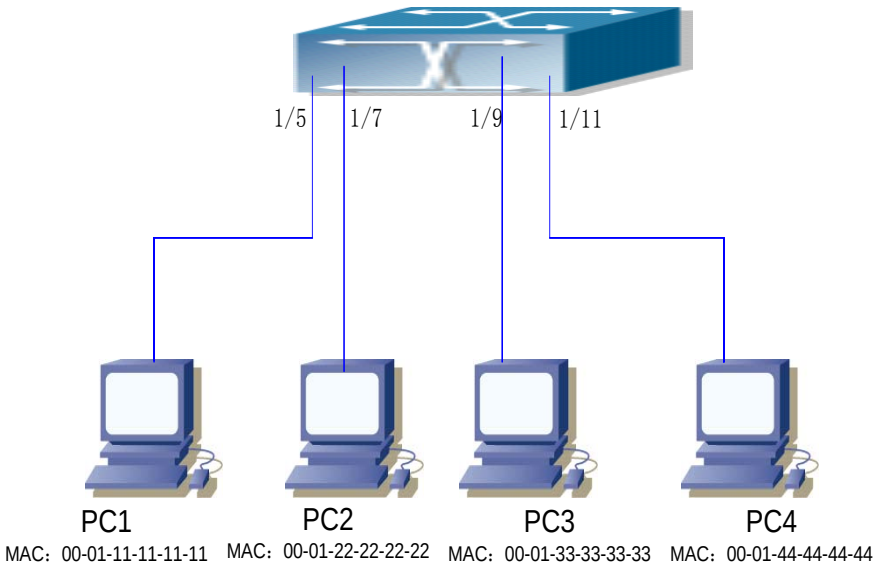


Fig 8-2 MAC Table typical configuration example

Scenario: Four PCs as shown in the above figure are connected to ports 1/5, 1/7, 1/9, 1/11 of ES4704BD, all the four PCs belong to the default VLAN1. As required by the network environment, dynamic learning is enabled. PC1 holds sensitive data and can not be accessed by any other PC that is in another physical segment; PC2 and PC3 have static mappings set to port 7 and port 9, respectively.

The configuration steps are listed below:

1. Set the MAC address 00-01-11-11-11-11 of PC1 as a filter address.

Switch(Config)#mac-address-table blackhole address 00-01-11-11-11-11 vlan 1

2. Set the static mapping relationship for PC2 and PC3 to port 7 and port 9, respectively.

Switch(Config)#mac-address-table static address 00-01-22-22-22-22 vlan 1 interface ethernet 1/7

Switch(Config)#mac-address-table static address 00-01-33-33-33-33 vlan 1 interface ethernet 1/9

8.4 Troubleshooting Help

8.4.1 Monitor and Debug Commands

8.4.1.1 show mac-address-table aging-time

Command: show mac-address-table aging-time

Function: Displays the aging time of dynamic MAC address entries in the switch MAC table.

Command mode: Admin Mode

Example: Displaying the current aging time of dynamic MAC address entries in the MAC table.

Switch#show mac-address-table **aging-time**

8.4.1.2 show mac-address-table static

Command: show mac-address-table [static] [address <*mac-addr*>] [vlan <*vlan-id*>] [interface <*interface-name*>]

Function: Displays the content of the current MAC table in the switch.

Parameters: static stands for static entries; **<*mac-addr*>** for the MAC addresses of the entries to be displayed; **<*vlan-id*>** for the VLAN numbers of the entries to be displayed; **<*interface-name*>** for the port names of the entries to be displayed

Command mode: Admin Mode

Default: MAC table content is not displayed by default.

Usage Guide: This command can be used to display static and dynamic MAC address entries in categorized view, you can also use the "**show mac-address-table**" command to display all MAC entries in the switch.

Example: Displaying the static entries in the MAC table.

Switch#show mac-address-table static

8.4.1.3 show mac-address-table blackhole

Command: show mac-address-table blackhole [address <*mac-addr*>] [vlan <*vlan-id*>]

Function: Displays the filter entries of the current MAC table.

Parameters: blackhole stands for filter entries; **<*mac-addr*>** for the MAC addresses of the entries to be displayed; **<*vlan-id*>** for the VLAN number of the entries to be displayed.

Command mode: Admin Mode

Default: Filter MAC entries are not displayed by default.

Usage Guide: This command can be used to display all filter MAC address entries in categorized view.

Example: Displaying the filter entries in the MAC table.

Switch#show mac-address-table blackhole

8.4.2 Troubleshooting Help

Using the show mac-address-table command, it has been discovered that a port has failed to learn the MAC of a device connected to it. Possible reasons:

- ☞ The connected cable is broken. Replace the cable.
- ☞ Spanning Tree has started and the port is in “discarding” status; or the device was recently connected to the port and Spanning Tree is still under calculation. Wait until the Spanning Tree calculation finishes. The port will then learn the MAC address.
- ☞ If not the above-mentioned problem, please check for port healthy and contact technical support for a solution.

8.5 MAC Address Function Extension

8.5.1 MAC Address Binding

8.5.1.1 Introduction to MAC Address Binding

Most switches support MAC address learning, allowing each port to dynamically learn several MAC addresses so that forwarding data streams between known MAC addresses within the ports can be achieved. If a MAC address has aged, the packet destined for that entry will be broadcasted. In other words, a MAC address learned in a port will be used for forwarding in that port, and if the connection has been changed to another port, the switch will learn the MAC address again to forward data in the new port.

However, in some cases, security or management policy may require MAC addresses to be bound with the ports, only data streams from the bound MAC are allowed to be forwarded in the ports. That is to say, after a MAC address is bound to a port, only the data streams destined for that MAC address can flow in from the binding port, data stream destined for the other MAC addresses

that are not bound to the port will not be allowed to pass through the port.

8.5.1.2 MAC Address Binding Configuration

8.5.1.2.1 MAC Address Binding Configuration Task Sequence

1. Enable MAC address binding function for the ports
2. Lock the MAC addresses for a port
3. MAC address binding property configuration

1. Enable MAC address binding function for the ports

Command	Explanation
Interface Mode	
switchport port-security **no switchport port-security**	Enables MAC address binding function for the port: the "**no switchport port-security"** command disables the MAC address binding function for the port**.**

2. Lock the MAC addresses for a port

Command	Explanation
Interface Mode	
switchport port-security lock **no switchport port-security lock**	Locks the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no switchport port-security lock"** command restores the MAC address learning function for the port.
switchport port-security convert	Converts dynamic secure MAC addresses learned by the port to static secure MAC addresses.
switchport port-security timeout <*value*> **no switchport port-security timeout**	Enables port locking timer function; the "**no switchport port-security timeout**" restores the default setting.
switchport port-security mac-address <*mac-address*> **no switchport port-security mac-address <*mac-address*>**	Adds static secure a MAC address; "**no switchport port-security mac-address"** command deletes static secure MAC address.
Admin Mode	
clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]	Clears dynamic MAC addresses learned by the specified port.

3. MAC address binding property configuration

Command	Explanation
Interface Mode	
switchport port-security maximum <*value*> **no switchport port-security maximum <*value*>**	Sets the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum**" command restores the default value.
switchport port-security violation {protect | shutdown} **no switchport port-security violation**	Sets the violation mode for the port; "**no switchport port-security violation**" command restores the default setting.

8.5.1.2.2 MAC Address Binding Configuration Commands

8.5.1.2.2.1 switchport port-security

Command: switchport port-security

no switchport port-security

Function: Enables the MAC address binding function for the port: the "**no switchport port-security"** command disables the MAC address binding function for the port**.**

Command mode: Interface Mode

Default: MAC address binding is not enabled by default.

Usage Guide: The MAC address binding function, Spanning Tree and Port Aggregation functions are mutually exclusive. Therefore, if the MAC binding function for a port is to be enabled, the Spanning Tree and Port Aggregation functions must be disabled, and the port enabling MAC address binding must not be a Trunk port.

Example: Enabling the MAC address binding function for port 1

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security

8.5.1.2.2.2 switchport port-security convert

Command: switchport port-security convert

Function: Converts dynamic secure MAC addresses learned by the port to static secure MAC addresses, and disables the MAC address learning function for the port.

Command mode: Interface Mode

Usage Guide: The port dynamic MAC convert command can only be executed after the secure port is locked. After this command has been executed, dynamic secure MAC addresses learned by the port will be converted to static secure MAC addresses. The command does not reserve configuration.

Example: Converting MAC addresses in port 1 to static secure MAC addresses.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security convert

8.5.1.2.2.3 switchport port-security lock

Command: switchport port-security lock

no switchport port-security lock

Function: Locks the port. When a port is locked, the MAC address learning function for the port will be disabled: the "**no switchport port-security lock"** command restores the MAC address learning function for the port.

Command mode: Interface Mode

Default: Ports are not locked by default.

Usage Guide: The port locking command can only be executed after MAC address binding function has been enabled. When the port locking command has been executed, the dynamic MAC learning function for the port will be disabled.

Example: Locking port1.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security lock

8.5.1.2.2.4 switchport port-security timeout

Command: switchport port-security timeout <*value*>

no switchport port-security timeout

Function: Sets the timer for port locking; the "**no switchport port-security timeout**" command restores the default setting.

Parameters: < *value*> is the timeout value, the valid range is 0 to 300 seconds..

Command mode: Interface Mode

Default: Port locking timer is not enabled by default.

Usage Guide: The port locking timer function is a dynamic MAC address locking function. MAC address locking and conversion of dynamic MAC entries to secure address entries will be performed on locking timer timeout. The MAC address binding function must be enabled prior to running this command.

Example: Setting port1's locking timer to 30 seconds.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)# switchport port-security timeout 30

8.5.1.2.2.5 switchport port-security mac-address

Command: switchport port-security mac-address <*mac-address*>

no switchport port-security mac-address <*mac-address*>

Function: Adds a static secure MAC address; the "**no switchport port-security mac-address"** command deletes a static secure MAC address.

Command mode: Interface Mode

Parameters: <*mac-address*> stands for the MAC address to be added/deleted.

Usage Guide: The MAC address binding function must be enabled before static secure MAC address can be added.

Example: Adding MAC 00-03-0F-FE-2E-D3 to port1.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security mac-address 00-03-0F-FE-2E-D3

8.5.1.2.2.6 clear port-security dynamic

Command: clear port-security dynamic [address <*mac-addr*> | interface <*interface-id*>]

Function: Clears the Dynamic MAC addresses of the specified port.

Command mode: Admin Mode

Parameters: <*mac-addr*> stands MAC address; **<*interface-id*>** for specified port number.

Usage Guide: The secure port must be locked before dynamic MAC clearing operation can be performed in a specified port. If no ports and MAC are specified, then all dynamic MAC addresses in all locked secure ports will be cleared; if only a port but no MAC address is specified, then all MAC addresses in the specified port will be cleared.

Example: Deleting all dynamic MAC addresses in port1.

Switch#clear port-security dynamic interface Ethernet 1/1

8.5.1.2.2.7 switchport port-security maximum

Command: switchport port-security maximum <*value*>

no switchport port-security maximum

Function: Sets the maximum number of secure MAC addresses for a port; the "**no switchport port-security maximum**" command restores the maximum secure address number to 1.

Command mode: Interface Mode

Parameters: < *value*> is the maximum for static secure MAC addresses, the valid range is 1 to 128.

Default: The default number of maximum port secure MAC addresses is 1.

Usage Guide: The MAC address binding function must be enabled before the maximum number of secure MAC addresses can be set. If the secure static MAC address number of the port is larger than

the maximum secure MAC address number set, the setting fails; extra secure static MAC addresses must be deleted, so that the secure static MAC address number is no larger than the maximum secure MAC address number for the setting to be successful.

Example: Setting the maximum secure MAC address number for port 1 to 4.

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security maximum 4

8.5.1.2.2.8 switchport port-security violation

Command: switchport port-security violation {protect | shutdown}

no switchport port-security violation

Function: Sets the violation mode for the port; the "**no switchport port-security violation**" command restores the violation mode to **protect**.

Command mode: Interface Mode

Parameters: "**protect**" for protect mode; "**shutdown**" to disable the violation mode.

Default: The default violation mode for the port "**protect**".

Usage Guide: The port violation mode can only be set after MAC address binding function is enabled. If the port violation mode is set to "**protect**" when the secure MAC address number exceeds maximum secure MAC address number set, only the dynamic MAC address learning ability is disabled; if the violation mode is set to "**shutdown**", then the port will be shutdown when the secure MAC address number exceeds maximum secure MAC address number set, the user can manually open the port by using the "**no shutdown**" command.

Example: Setting the violation mode for port1 to "**shutdown**".

Switch(Config)#interface Ethernet 1/1

Switch(Config-Ethernet1/1)#switchport port-security violation shutdown

8.5.1.3 Mac Address Binding Troubleshooting Help

8.5.1.3.1 MAC Address Binding Debug and Monitor Commands

8.5.1.3.1.1 show port-security

Command: show port-security

Function: displays the global configuration of secure ports.

Command mode: Admin Mode

Default: Configuration of secure ports is not displayed by default.

Usage Guide: This command displays the information for ports that are currently configured as secure ports.

Example:

```
Switch#show port-security
Security Port       MaxSecurityAddr CurrentAddr       Security Action
                        (count)          (count)
-------------------------------------------------------------------------------------------------
 Ethernet1/3              128              0                  Protect
-------------------------------------------------------------------------------------------------
Max Addresses limit per port :128
Total Addresses in System :0
```

Displayed information	Explanation
Security Port	Name of port that is configured as a secure port.
MaxSecurityAddr	The maximum number of secure MAC addresses set for the secure port.
CurrentAddr	Current number of secure MAC addresses for the secure port.
Security Action	Violation mode set for the port.
Max Addresses limit per port	Maximum number of secure MAC addresses set for each secure port.
Total Addresses in System	Current number of secure MAC addresses in the system.

8.5.1.3.1.2 show port-security interface

Command: show port-security interface <*interface-id*>

Function: displays the configuration of secure port.

Command mode: Admin Mode

Parameters: <*interface-list*> stands for the port to be displayed.

Default: Configuration of secure ports is not displayed by default.

Usage Guide: This command displays the detailed configuration information for the secure port.

Example:

```
Switch#show port-security interface ethernet 1/1
Ethernet1/1 Port Security :Enabled
Port status :Security Up
Violation mode :Protect
Maximum MAC Addresses :1
Total MAC Addresses :1
```

Configured MAC Addresses :1

Lock Timer is ShutDown

Mac-Learning function is: Enabled

Displayed information	Explanation
Port Security	Is port enabled as a secure port?
Port status	Port secure status
Violation mode	Violation mode set for the port.
Maximum MAC Addresses	The maximum number of secure MAC addresses set for the port
Total MAC Addresses	Current number of secure MAC addresses for the port.
Configured MAC Addresses	Current number of secure static MAC addresses for the port.
Lock Timer	Tells if locking timer (timer timeout) is enabled or disable for the port.
Mac-Learning function	Is the MAC address learning function enabled?

8.5.1.3.1.3 show port-security address

Command: show port-security address [interface <*interface-id*>]

Function: Displays the secure MAC addresses of the port.

Command mode: Admin Mode

Parameters: <*interface-list*> stands for the port to be displayed.

Usage Guide: This command displays the secure port MAC address information, if no port is specified, secure MAC addresses of all ports are displayed.

Example:

Switch#show port-security address interface ethernet 1/3

Ethernet1/3 Security Mac Address Table

Vlan	Mac Address	Type	Ports
1	0000.0000.1111	SecureConfigured	Ethernet1/3

Total Addresses :1

Displayed information	Explanation
Vlan	VLAN ID for the secure MAC Address
Mac Address	Secure MAC address
Type	Secure MAC address type

Ports	The ports that the secure MAC addresses belongs to
Total Addresses	Current number of secure MAC address in the system.

8.5.1.3.2 MAC Address Binding Troubleshooting Help

Enabling MAC address binding for ports may fail on some occasions. Here are some possible causes and solutions:

- ☞ If MAC address binding cannot be enabled for a port, make sure the port is not executing Spanning tree, port aggregation and is not configured as a Trunk port. MAC address binding is exclusive to such configurations. If MAC address binding is to be enabled, the above-mentioned functions must be disabled first.
- ☞ If a secure address is set as a static address and deleted, than that secure address will be unusable even though it no longer exists. For this reason, it is recommended to avoid static address for ports enabling MAC address binding.

8.6 WEB MANAGEMENT

Click “MAC address table configuration” to open MAC address configuration management list. Users can proceed to manage, set security port, add and delete MAC addresses, and so on.

8.6.1 Mac address table configuration

Click “MAC address table configuration”, to open MAC address list configuration management list to manage add delete MAC addresses.

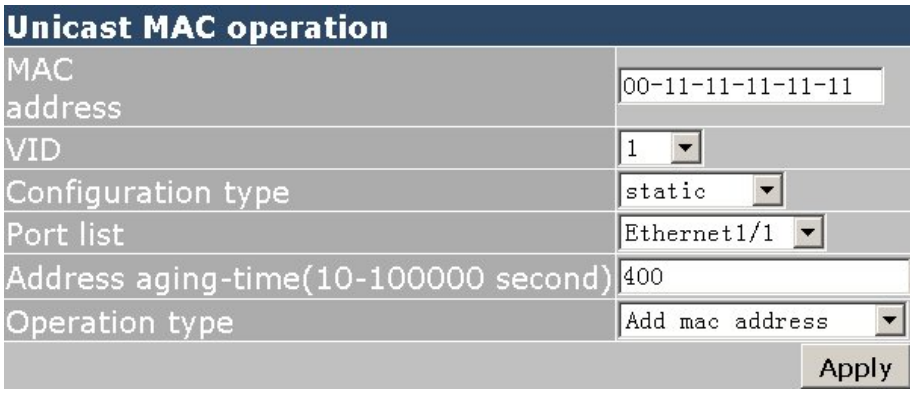
8.6.1.1 Unicast address configuration

Click “MAC address table configuration”, “MAC address table configuration”, “unicast address configuration”, “unicast address configuration” to add MAC addresses. Equals to CLI command 8.2.2：

- MAC address: Specifies a MAC address
- VID: The VLAN number of the MAC address
- Configuration type: static means static address; blackhole means filter address
- Port list: MAC address’s port
- Address aging-time: Aging time of dynamic MAC addresses
- Operation type: adds/deletes a MAC address

Example:

Set up MAC address as 00-11-11-11-11-11, select VID as 1, configuration type as static; port list as Ethernet 1/1 and address aging-time as 400 seconds. Select operation type as add mac address and click Apply button. Then the set up will be applied to port 1/1.

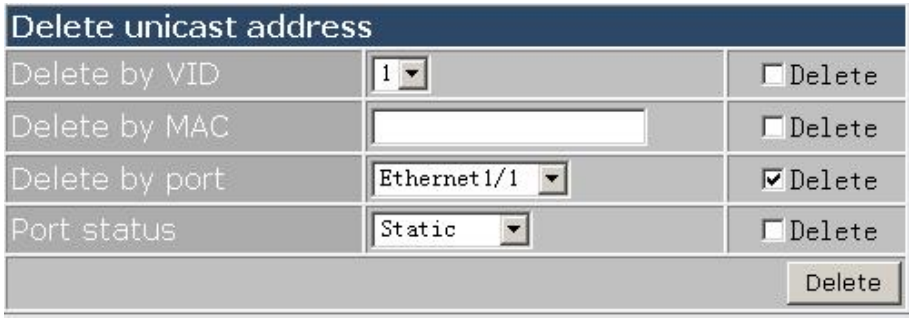


8.6.1.2 Delete unicast address

Click "MAC address table configuration", "MAC address table configuration", to delete a unicast address and MAC address. Equals to CLI command 8.2.2:

- Delete by VID: Deletes static MAC by the specified VID. Select Delete button to confirm the action
- Delete by MAC: Deletes specify MAC address. Select Delete button to confirm the action.
- Delete by port: Deletes MAC by port, select the Delete button to confirm the action
- Port status: select from Static address, dynamic address, and always filter. Select the Delete button to confirm deleting MAC according to MAC type

Example: Select VID as 1, select port as Ethernet1/1; port status as Static and click Delete button, then will delete all static MAC address in port 1/1.

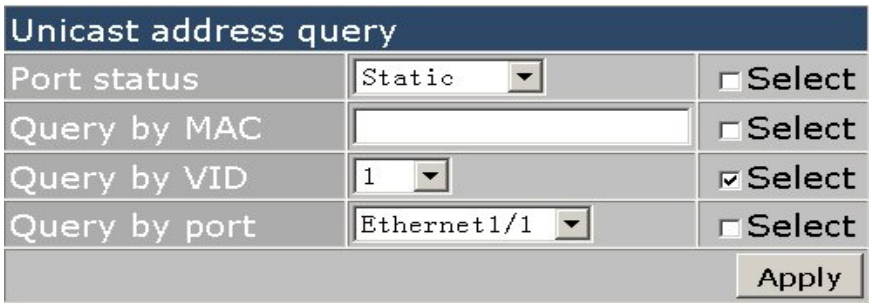


8.6.1.3 MAC address query

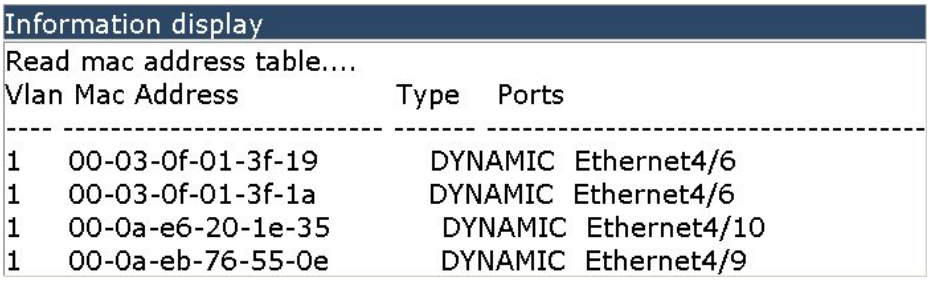
- Click "MAC address table configuration", "MAC address table configuration", "MAC address query" to do MAC address query. Equals to CLI command 8.4.1.1:
- Query by VID: Search static MAC addresses by specified VID. Select Search button to confirm the action.

- Query by MAC: Search by MAC address, select Search button to confirm the action
- Query by port: Search MAC by specified port. Select Search button to confirm the action
- Port status: select from Static address, dynamic address, and always filter. Select Search button to confirm search MAC according to MAC type.

Example: Select VID 1 and select query by VID. Click Search starting query.

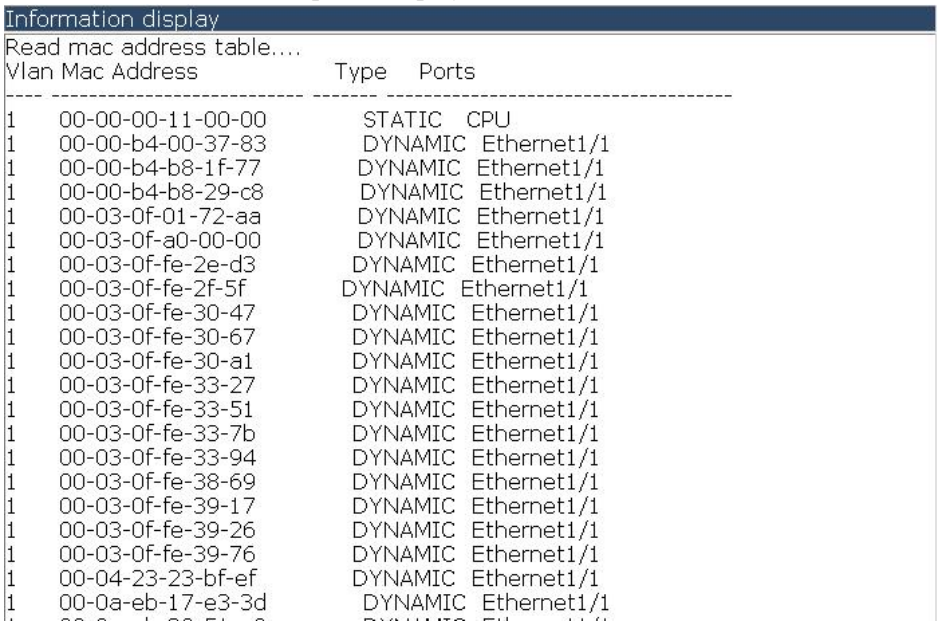


The new page will show the query results



8.6.1.4 Show MAC address table

Click "MAC address table configuration", "MAC address table configuration", "show mac-address-table" to show current MAC address information of the switch. Equals to CLI command 8.4.1.1. An example of displayed information is as follows:


Information display
Read mac address table....
Vlan Mac Address Type Ports
1 00-00-00-11-00-00 STATIC CPU
1 00-00-b4-00-37-83 DYNAMIC Ethernet1/1
1 00-00-b4-b8-1f-77 DYNAMIC Ethernet1/1
1 00-00-b4-b8-29-c8 DYNAMIC Ethernet1/1
1 00-03-0f-01-72-aa DYNAMIC Ethernet1/1
1 00-03-0f-a0-00-00 DYNAMIC Ethernet1/1
1 00-03-0f-fe-2e-d3 DYNAMIC Ethernet1/1
1 00-03-0f-fe-2f-5f DYNAMIC Ethernet1/1
1 00-03-0f-fe-30-47 DYNAMIC Ethernet1/1
1 00-03-0f-fe-30-67 DYNAMIC Ethernet1/1
1 00-03-0f-fe-30-a1 DYNAMIC Ethernet1/1
1 00-03-0f-fe-33-27 DYNAMIC Ethernet1/1
1 00-03-0f-fe-33-51 DYNAMIC Ethernet1/1
1 00-03-0f-fe-33-7b DYNAMIC Ethernet1/1
1 00-03-0f-fe-33-94 DYNAMIC Ethernet1/1
1 00-03-0f-fe-38-69 DYNAMIC Ethernet1/1
1 00-03-0f-fe-39-17 DYNAMIC Ethernet1/1
1 00-03-0f-fe-39-26 DYNAMIC Ethernet1/1
1 00-03-0f-fe-39-76 DYNAMIC Ethernet1/1
1 00-04-23-23-bf-ef DYNAMIC Ethernet1/1
1 00-0a-eb-17-e3-3d DYNAMIC Ethernet1/1

8.6.2 MAC address binding configuration

Click “MAC address table configuration”, “MAC address binding configuration”, to open MAC address binding configuration list to setup the port security function.

8.6.2.1 Enable port MAC-Binding

Click “MAC address table configuration”, “MAC address binding configuration”, “Enable port Mac-binding”, to enable port MAC-binding list to set up port security function.

8.6.2.1.1 Enable port MAC-Binding

Click “MAC address table configuration”, “MAC address binding configuration”, “Enable port Mac-binding”, “Enable port Mac-binding” to enable and disable the port MAC-binding function. Equals to CLI command 8.5.1.2.2.1

- Port: specify configuration port

Select port as Ethernet 1/1 and click Apply button to enable the port MAC binding function on Ethernet 1/1

8.6.2.2 Lock port

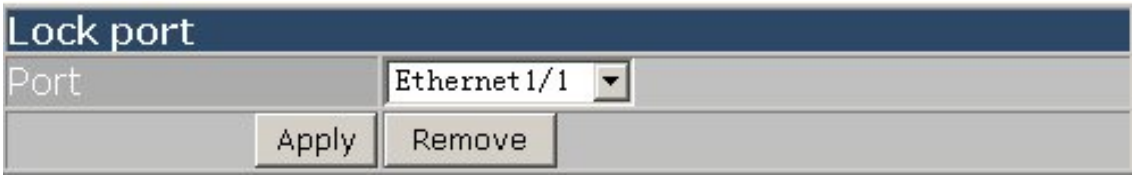
Click “MAC address table configuration”, “MAC address binding configuration”, “Lock port” to enable the lock port configuration list to set up port security functions including lock port, MAC converting, and so on.

8.6.2.2.1 Lock port

Click “MAC address table configuration”, “MAC address binding configuration”, “Lock port”, “Lock port” to lock ports. Equals to CLI command 8.5.1.2.2.3

- Port: specify configuration port

Select port as Ethernet1/1 and click Apply button to lock Ethernet port 1/1

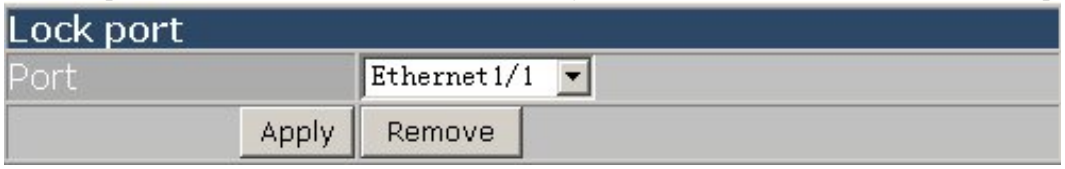


8.6.2.2.2 Dynamic MAC converting

Click “MAC address table configuration”, “MAC address binding configuration”, “lock port”, “dynamic mac converting” to convert the dynamic mac addresses, which were learned by the ports, to static security mac addresses. Equals to cli command.5.1.2.2.2

- Port: specifies configuration port

Example: Select Ethernet port 1/1 and click Apply button, then the dynamic MAC addresses of Ethernet port 1/1 will be converted to static security MAC addresses. Click Reset to reselect port.



8.6.2.2.3 Enable port security timeout

Click “MAC address table configuration”, “MAC address binding configuration”, “Lock port”, “Enable port security timeout” to lock port security. Equals to CLI command 8.5.1.2.2.4:

- Port: specifies the configuration port
- Timeout Value (0-300 seconds): Lock the time out value

Example: Select Ethernet port 1/1 and set up Timeout value as 30 seconds, then click the Apply button. The Ethernet port 1/1 security timeout will then be 30 seconds

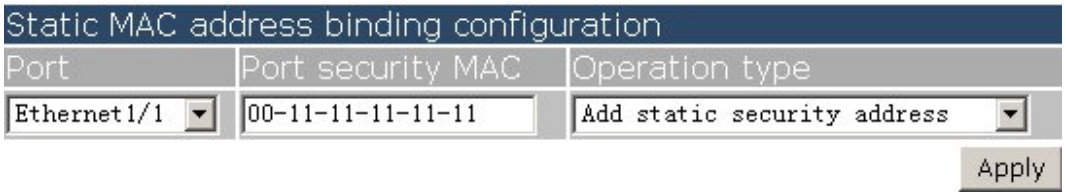
8.6.2.2.4 Binding MAC

Click “MAC address table configuration”, “MAC address binding configuration”, “Lock port”, “Binding MAC”, to add/remove static security MAC addresses. Equals to CLI command 8.5.1.2.2.5

- Port: Specifies the port
- Port security MAC: MAC address

Operation type: adds/removes static security addresses.

Example: Select Ethernet Port 1/1 and assign MAC as 00-11-11-11-11-11, select add static security address then click the Apply button to apply this setting to the switch.

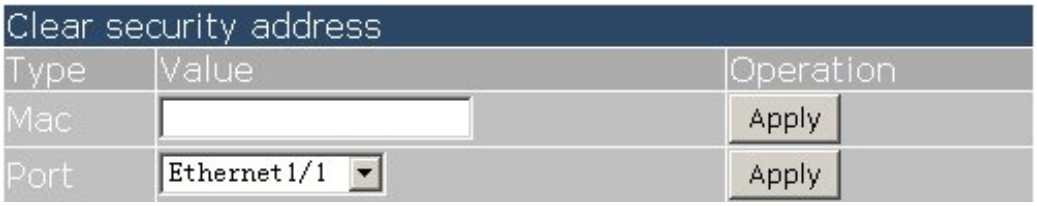


8.6.2.2.5 Clearing port MAC

Click “MAC address table configuration”, “MAC address binding configuration”, “Lock port”, “Clearing port MAC” to clear the dynamic MAC addresses of the selected port. Equals to CLI command 8.5.1.2.2.6.

- Mac: Specifies the deleted MAC
- Port: Specifies the port to delete MAC

Example: Select Ethernet port 1/1 and click the Apply button then the dynamic MAC of Ethernet port 1/1 will be deleted.



8.6.2.3 MAC binding attribution configuration

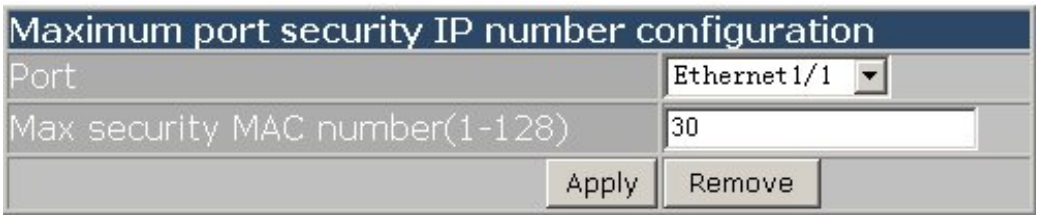
Click “MAC address table configuration”, “MAC address binding configuration”, “MAC binding attribution configuration” to enable port security configuration management lists to set up port security types.

8.6.2.3.1 Maximum port security IP number configuration

Click “MAC address table configuration”, “MAC address binding configuration”, “MAC binding attribution configuration”, “Maximum port security IP number configuration” to set up the maximum port security MAC address numbers. Equals to CLI command 8.5.1.2.2.7.

- Port: Specifies the port
- Max security MAC number (1-128): Maximum port security MAC address number.

Select Ethernet port 1/1 and set up Max security MAC number as 30,nd click Apply button to apply this setting to the switch.



8.6.2.3.2 Port violation mode

Click “MAC address table configuration”, “MAC address binding configuration”, MAC binding attribution configuration, Port violation mode to set up port security violation mode. Equals to CLI command 8.5.1.2.2.8.

- Port: Specify port
- Violation mode: Port violation mode and is divided into Protect and shutdown modes.

Select Ethernet port 1/1 , select violation mode as protect and click Apply button and apply this setting to the switch.

8.6.2.4 MAC binding debug

Click “MAC address table configuration”, “MAC address binding configuration”, “MAC binding debug” to open port security debug window to check port security debugging information.

8.6.2.4.1 Show MAC binding security address

Click “MAC address table configuration”, “MAC address binding configuration”, “MAC binding debug”, “Show mac binding security address” to check port security related information.

- Show port-security by interface: displays the specified port security configuration status. Equals to CLI command 8.5.1.3.1.3.
- Show port-security address by interface: displays the specified port security MAC address. Equals to CLI command 8.5.1.3.1.3.
- Show all port-security: displays all port security configuration status. Equals to CLI command 8.5.1.3.1.1.
- Show all port-security address: displays all port security MAC addresses. Equals to CLI command 8.5.1.3.1.2

Click Show all port-security address to display port security configuration status.

Information Display will show the results.

Information display
Security Mac Address Table
Vlan Mac Address Type Ports
Total Addresses in System :0
Max Addresses limit in System :128

Chapter 9 VLAN Configuration

9.1 Introduction to VLAN

VLAN (Virtual Local Area Network) is a technology that divides the logical addresses of devices within the network to separate network segments based on functions, applications or management requirements. This way, virtual workgroups can be formed regardless of the physical location of the devices. IEEE 802.1Q protocol was announced to direct the standardized VLAN implementation. ES4704BD VLAN implementation follows IEEE 802.1Q.

VLAN technology can partition a big LAN into many separate broadcast domains dynamically to meet demands.

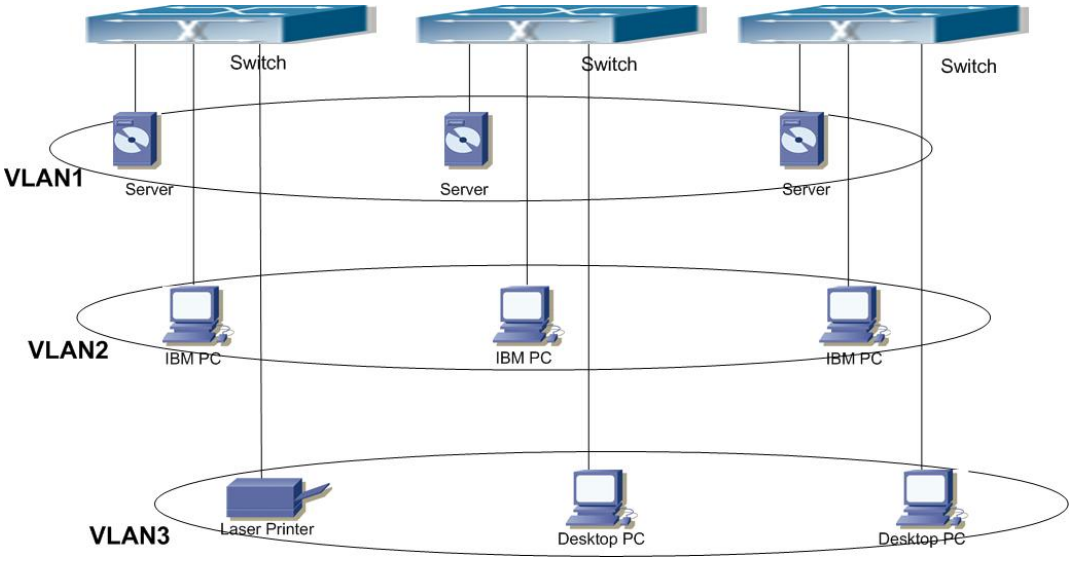


Fig 9-1 VLAN network defined logically

Each broadcast domain is a VLAN. VLANs have the same properties as the physical LANs, except VLAN are a logically partitioned rather than physical. Therefore, the partition of VLANs can be performed regardless of physical locations. Furthermore, broadcast, multicast and unicast traffic within a VLAN are separated from other VLANs.

With the afore-mentioned features, VLAN technology provides us with the following conveniences:

- Improved network performance
- Savings on network resources
- Simplified Network Management
- Lowered network cost
- Enhanced network security

VLAN and GVRP (GARP VLAN Registration Protocol) are defined by IEEE 802.1Q and

implemented by ES4704BD. This chapter will describe the use and configuration of VLANs and GVRP in detail.

9.2 VLAN Configuration

9.2.1 VLAN Configuration Task Sequence

1. Creating or deleting VLAN
2. Specifying or deleting VLAN name
3. Assigning Switch ports for VLAN
4. Setting the port type for the switch
5. Setting Trunk port
6. Setting Access port
7. Enabling/Disabling VLAN ingress rules on ports

1. Creating or deleting VLAN

Command	Explanation
Global Mode	
vlan <*vlan-id*> **no vlan <*vlan-id*>**	Creates/deletes a VLAN or enters VLAN Mode

2. Specifying or deleting VLAN name

Command	Explanation
VLAN Mode	
name <*vlan-name*> **no name**	Sets or deletes a VLAN name

3. Assigning Switch ports for VLAN

Command	Explanation
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Assigns Switch ports to a VLAN

4. Set The Switch Port Type

Command	Explanation
Interface Mode	
switchport mode {trunk|access}	Sets the current port as a Trunk or Access port.

5. Set Trunk port

Command	Explanation
Interface Mode	
switchport trunk allowed vlan {<*vlan-list*>|all} **no switchport trunk allowed vlan**	Sets/deletes VLAN allowed to be crossed by Trunk.
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Sets/deletes PVID for Trunk port.

6. Set Access port

Command	Explanation
Interface Mode	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Adds the current port to specified VLAN or exits the specified VLANs.

7. Disable/Enable VLAN Ingress Rules

Command	Explanation
Global Mode	
vlan ingress disable **no vlan ingress enabledisable**	Disables/Enable VLAN ingress rules

9.2.2 VLAN Configuration Commands

9.2.2.1 vlan

Command: vlan <*vlan-id*>

no vlan <*vlan-id*>

Function: Creates a VLAN and enters VLAN configuration mode. In VLAN Mode, the user can configure a VLAN name and the switch ports assigned to the VLAN. The "**no vlan <*vlan-id*>**" command deletes specified VLANs.

Parameters: <*vlan-id*> is the VLAN ID to be created/deleted, valid range is 1 to 4094.

Command mode: Global Mode

Default: VLAN1 is set by default.

Usage Guide: VLAN1 is the default VLAN and cannot be configured or deleted by the user. The

allowed VLAN number is 4094. It should be noted that dynamic VLANs learnt by GVRP cannot be deleted by this command.

Example: Creating VLAN 100 and entering the configuration mode for VLAN 100.

Switch(Config)#vlan 100

Switch(Config-Vlan100)#

9.2.2.2 name

Command: name <*vlan-name*>

no name

Function: Specifies a name for VLAN, a VLAN name is a descriptive string corresponding to the VLAN. The "**no name**" command deletes the VLAN name.

Parameters: <*vlan-name*> is the specified VLAN name string.

Command mode: VLAN Mode

Default: The default VLAN name is "vlanXXX", where XXX is the VID.

Usage Guide: The switch provides a function to specify different names for different VLANs, this can make VLAN naming easier to remember and manage.

Example: Specifying the name for VLAN100 to be TestVlan.

Switch(Config-Vlan100)#name TestVlan

9.2.2.3 switchport access vlan

Command: switchport access vlan <*vlan-id*>

no switchport access vlan

Function: Adds the current Access port to the specified VLAN, the "**no switchport access vlan**" command deletes the current port from the specified VLAN, and the port will be partitioned to VLAN1.

Parameters: <*vlan-id*> is the VID for the VLAN to add current port, valid range is 1 to 4094.

Command mode: Interface Mode

Default: All ports belong to VLAN1 by default.

Usage Guide: Only ports in Access mode can join specified VLANs, and an Access port can only join one VLAN at a time.

Example: Adding a Access port to VLAN100.

Switch(Config)#interface ethernet 1/8

Switch(Config-ethernet1/8)#switchport mode access

Switch(Config-ethernet1/8)#switchport access vlan 100

Switch(Config-ethernet1/8)#exit

9.2.2.4 switchport interface

Command: switchport interface <*interface-list*>

no switchport interface <*interface-list*>

Function: Assigns Ethernet ports to VLAN; the "**no switchport interface <*interface-list*>**" command deletes one or one set of ports from the specified VLAN.

Parameters: <*interface-list*> is the port list to be added or deleted, ";" and "-" are supported, for **example:** ethernet 1/1;2;5 or ethernet 1/1-6;8.

Command mode: VLAN Mode

Default: A newly created VLAN contains no ports by default.

Usage Guide: Access ports are normal ports and can join a VLAN, but a port can only join one VLAN for at a time.

Example: Assigning Ethernet ports 1, 3, 4-7, 8 of slot 1 to VLAN100.

Switch(Config-Vlan100)#switchport interface ethernet 1/1;3;4-7;8

9.2.2.5 switchport mode

Command: switchport mode {trunk|access}

Function: Sets the port in access mode or trunk mode.

Parameters: trunk means the port allows traffic of multiple VLANs; **access** indicates the port belongs to one VLAN only.

Command mode: Interface Mode

Default: The port is in Access mode by default.

Usage Guide: Ports in trunk mode are called Trunk ports. Trunk ports can allow traffic of multiple VLANs to pass through, VLANs in different switches can be interconnected with the Trunk port interconnections. Ports under access mode are called Access ports. An access port can be assigned to one and only one VLAN at a time.

Example: Setting port 1/5 to trunk mode and port 1/8 to access mode.

Switch(Config)#interface ethernet 1/5

Switch(Config-ethernet1/5)#switchport mode trunk

Switch(Config-ethernet1/5)#exit

Switch(Config)#interface ethernet 1/8

Switch(Config-ethernet1/8)#switchport mode access

Switch(Config-ethernet1/8)#exit

9.2.2.6 switchport trunk allowed vlan

Command: switchport trunk allowed vlan {<*vlan-list*>|all}

no switchport trunk allowed vlan

Function: Sets trunk port to allow VLAN traffic; the "**no switchport trunk allowed vlan**" command restores the default setting.

Parameters: <*vlan-list*> is the list of VLANs allowed to pass through in the specified Trunk port; keyword "**all"** allows all VLAN traffic on the Trunk port.

Command mode: Interface Mode

Default: Default is Trunk port allowing all VLAN traffic

Usage Guide: The user can use this command to allow VLAN traffic to pass though the trunk port; traffic of VLANs not included are prohibited.

Example: Setting the Trunk port to allow traffic of VLAN1, 3, 5-20.

Switch(Config)#interface ethernet 1/5

Switch(Config-ethernet1/5)#switchport mode trunk

Switch(Config-ethernet1/5)#switchport trunk allowed vlan 1;3;5-20

Switch(Config-ethernet1/5)#exit

9.2.2.7 switchport trunk native vlan

Command: switchport trunk native vlan <*vlan-id*>

no switchport trunk native vlan

Function: Sets the PVID for Trunk port; the "**no switchport trunk native vlan**" command restores the default setting.

Parameters: <*vlan-id*> is the PVID for Trunk port.

Command mode: Interface Mode

Default: The default PVID of Trunk port is 1.

Usage Guide: PVID concept is defined in IEEE 802.1Q. PVID of Trunk ports are used to tag untagged frames. When a untagged frame enters a Trunk port, the port will tag the untagged frame with the native PVID set with this command for VLAN forwarding.

Example: Setting the native vlan for a Trunk port to 100.

Switch(Config)#interface ethernet 1/5

Switch(Config-ethernet1/5)#switchport mode trunk

Switch(Config-ethernet1/5)#switchport trunk native vlan 100

Switch(Config-ethernet1/5)#exit

9.2.2.8 vlan ingress disable

Command: vlan ingress disable

no vlan ingress disable

Function: Disables the VLAN ingress rule for a port; the "**no vlan ingress disable**" command enables the ingress rule.

Command mode: Interface Mode

Default: VLAN ingress rules are enabled by default.

Usage Guide: When VLAN ingress rules are enabled on the port and the system receives data, it will check the source port first, then forwards the data to the destination port if it is a VLAN member port.

Example: Disabling the VLAN ingress rules on the port

Switch(Config-Ethernet1/1)# vlan ingress disable

9.2.3 Typical VLAN Application

Scenario:

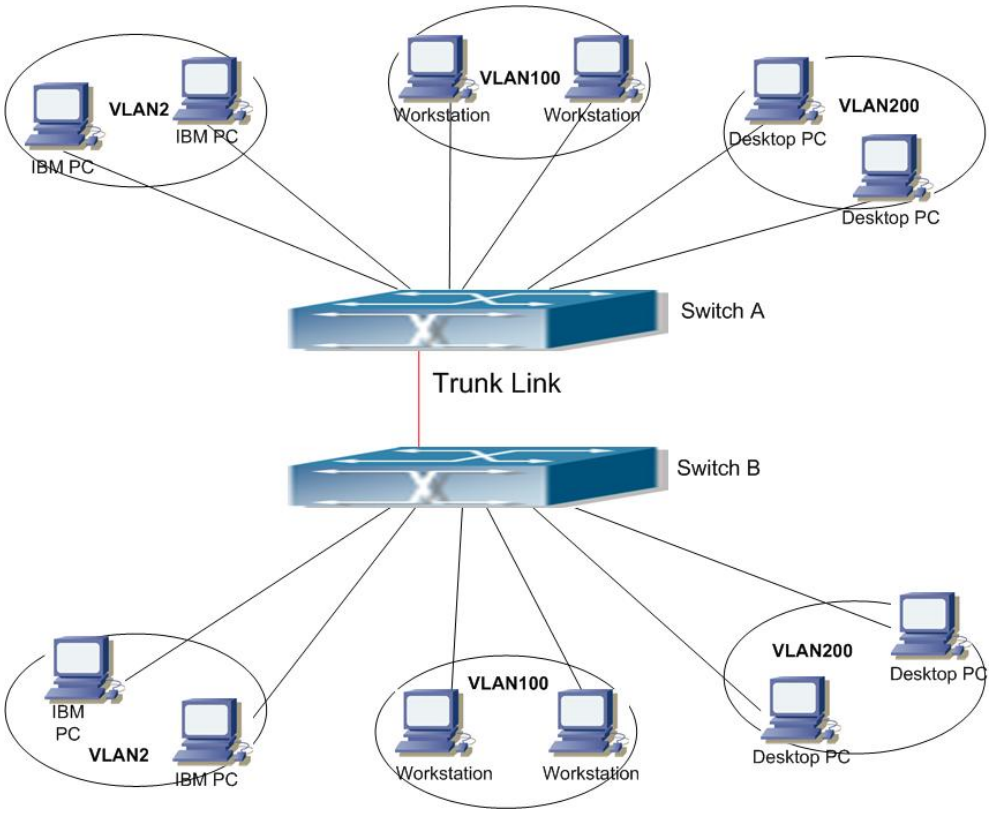


Fig 9-2 Typical VLAN Application Topology

Example: The existing LAN is required to be partitioned to 3 VLANs due to security and application requirements. The three VLANs are VLAN2, VLAN100 and VLAN200. These three VLANs must cross location A and B. One switch is placed in each site, and the cross-location requirement can be met if VLAN traffic can be transferred between the two switches.

Configuration Item	Configuration description
VLAN2	Site A and site B switch port 2 – 4.
VLAN100	Site A and site B switch port 5 – 7.
VLAN200	Site A and site B switch port 8 – 10.
Trunk port	Site A and site B switch port 11 .

Connect the Trunk ports of both switches for a Trunk link to convey the cross-switch VLAN traffic. Connect all network devices to the other ports of the corresponding VLANs.

In this example, port 1 and port 12 are not assigned and so can be used as management ports or for other purposes.

The configuration steps are listed below:

Switch A:

```
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#exit
Switch(Config)#
```

Switch B:

```
Switch(Config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/2-4
Switch(Config-Vlan2)#exit
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/5-7
Switch(Config-Vlan100)#exit
Switch(Config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/8-10
Switch(Config-Vlan200)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#exit
```

9.3 GVRP Configuration

GARP (Generic Attribute Registration Protocol) can be used to dynamically distribute, populate and register property information between switch members within a switch network, the property can be VLAN information, Multicast MAC address of the other information. As a matter of fact, GARP protocol can convey multiple property features the switch needs to populate. Various GARP applications are defined on the basis of GARP, which are called GARP application entities, and GVRP is one of them.

GVRP (GARP VLAN Registration Protocol) is an application based on GARP working mechanism. It is responsible for the maintenance of dynamic VLAN register information and population of such register information to the other switches. Switches supporting GVRP can receive dynamic VLAN register information from the other switches, and update local VLAN register information according the information received. A GVRP enabled switch can also populate their own VLAN register information to the other switches. The VLAN register information populated includes local static information manually configured and dynamic information learnt from the other switches. Therefore, by populating the VLAN register information, VLAN information consistency can be achieved among all GVRP enabled switches.

9.3.1 GVRP Configuration Task Sequence

1. Configuring GARP Timer Parameters.
2. Enabling GVRP function

1. Configuring GARP Timer parameters.

Command	Explanation
Interface Mode	
garp timer join <*timer-value*> **no garp timer join** **garp timer leave <*timer-value*>** **no garp timer leave** **garp timer hold <*timer-value*>** **no garp timer hold**	Configures the hold, join and leave timers for GARP.
Global Mode	
garp timer leave all <*timer-value*> **no garp timer leave all**	Configures the leave all timer for GARP.

2. Enable GVRP function

Command	Explanation
Interface Mode	
gvrp **no gvrp**	Enables the GVRP function on current port.
Global Mode	
gvrp **no gvrp**	Enables the GVRP function for the switch.

9.3.2 GVRP Commands

9.3.2.1 garp timer join

Command: garp timer join <*timer-value*>

no garp timer join

Function: Sets the **join** timer for GARP; the " **no garp timer join**" command restores the default timer setting.

Parameters: < *timer-value*> is the value for **join** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for **join** timer is 200 ms.

Usage Guide: GARP application entity sends a **join** message after **join** time times out, other GARP application entities will register this message sent by this GARP application entity upon receiving the **join** message.

Example: Setting the GARP **join** timer value of port 1/10 to 1000 ms.

Switch(Config-Ethernet1/10)#garp timer join 1000

9.3.2.2 garp timer leave

Command: garp timer leave <*timer-value*>

no garp timer leave

Function: Sets the **leave** timer for GARP; the " **no garp timer leave**" command restores the default timer setting.

Parameters: < *timer-value*> is the value for **leave** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for **leave** timer is 600 ms.

Usage Guide: When GARP application entity wants to cancel a certain property information, it sends a **leave** message. GARP application entities receiving this message will start the **leave** timer, if no **join** message is received before the **leave** timer times out, the property information will be canceled. Note: the value of **leave** timer must be larger than twice of **join** timer, otherwise a error message will be displayed.

Example: Setting the GARP **leave** timer value of port 1/10 to 3000 ms.

Switch(Config-Ethernet1/10)#garp timer leave 3000

9.3.2.3 garp timer hold

Command: garp timer hold <*timer-value*>

no garp timer hold

Function: Sets the **hold** timer for GARP; the "**no garp timer hold**" command restores the default timer setting.

Parameters: < *timer-value*> is the value for GARP **hold** timer, the valid range is 100 to 327650 ms.

Command mode: Interface Mode

Default: The default value for **hold** timer is 100 ms.

Usage Guide: When GARP application entities receive a **join** message, **join** message will not be sent immediately. Instead, **hold** timer is started. After **hold** timer times out, all **join** messages received within the hold time will be sent in one GVRP frame, thus effectively reducing protocol message traffic.

Example: Setting the GARP **hold** timer value of port 1/10 to 500 ms.

Switch(Config-Ethernet1/10)#garp timer hold 500

9.3.2.4 garp timer leaveall

Command: garp timer leaveall <*timer-value*>

no garp timer leaveall

Function: Sets the **leaveall** timer for GARP; the " **no garp timer leaveall**" command restores the default timer setting.

Parameters: < *timer-value*> is the value for GARP **leaveall** timer, the valid range is 100 to 327650 ms.

Command mode: Global Mode

Default: The default value for **leaveall** timer is 10000 ms.

Usage Guide: When a GARP application entity starts, the **leaveall** timer is started at the same time. When **leaveall** timer times out, the GARP application entity will send a **leaveall** message. Other application entities will cancel all property information for that application entity, and the **leaveall** timer is cleared for a new cycle.

Example: Setting the GARP **leaveall** timer value to 50000 ms.

Switch(Config)#garp timer leaveall 50000

9.3.2.5 gvrp

Command: gvrp

no gvrp

Function: Enables the GVRP function for the switch or the current Trunk port; the "**no gvrp"** command disables the GVRP function globally or for the port**.**

Command mode: Interface Mode and Global Mode.

Default: GVRP is disabled by default.

Usage Guide: Port GVRP can only be enabled after global GVRP is enabled. When global GVRP is disabled, port GVRP configurations are also void. Note GVRP can only be enabled on Trunk ports.

Example: Enabling the GVRP function globally and for Trunk port 1/10.

Switch(Config)#gvrp

Switch(Config)#interface ethernet 1/10

Switch(Config-Ethernet1/10)#gvrp

Switch(Config)#exit

9.3.3 Typical GVRP Application

Scenario:

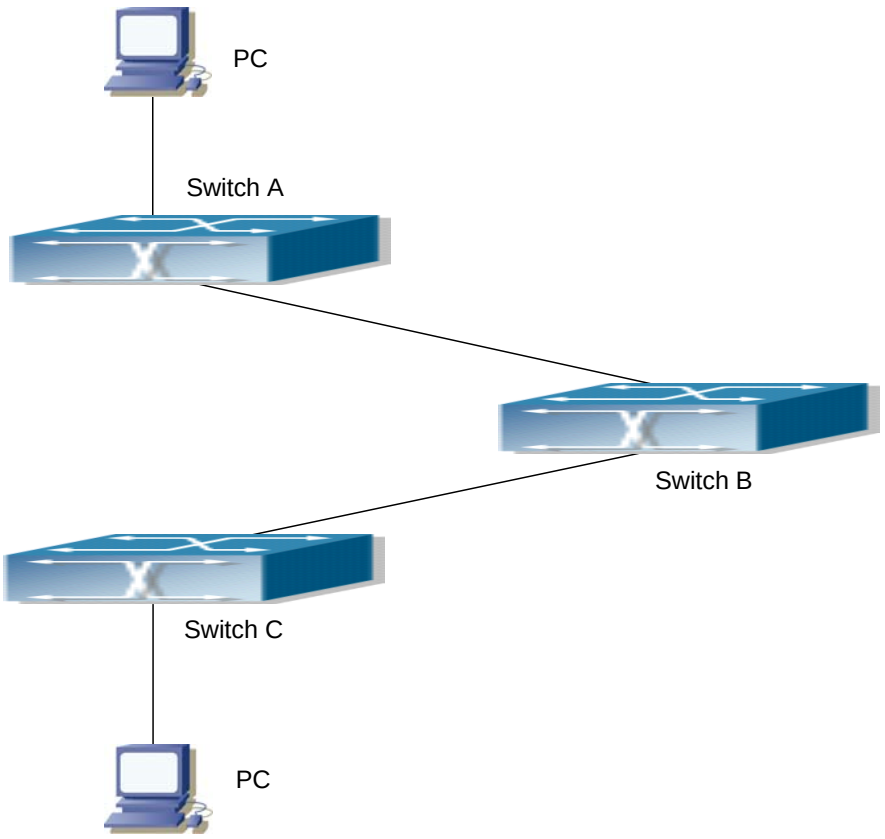


Fig 9-3 Typical GVRP Application Topology

Example: To enable dynamic VLAN information register and update among switches, GVRP protocol is configured in the switch. Configure GVRP in Switch A, B and C, enable Switch B to learn VLAN100 dynamically so that the two workstation connected to VLAN100 in Switch A and C can communicate with each other through Switch B without static VLAN100 entries.

Configuration Item	Configuration description
VLAN100	Port 2 – 6 of Switch A and C
Trunk port	Port 11 of Switch A and C, Port 10, 11 of Switch B
Global GVRP	Switch A, B, C:
Port GVRP	Port 11 of Switch A and C, Port 10, 11 of Switch B

Connect the two workstation to the VLAN100 ports in switch A and B, connect port 11 of Switch A to port 10 of Switch B, and port 11 of Switch B to port 11 of Switch C. All ports are on slots 1 of Switch A, B and C.

The configuration steps are listed below:

Switch A:

```
Switch(Config)#gvrp
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
Switch(Config-Vlan100)#exit
Switch(Config)#interface Ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#gvrp
Switch(Config-Ethernet1/11)#exit
```

Switch B:

```
Switch(Config)#gvrp
Switch(Config)#interface ethernet 1/10
Switch(Config-Ethernet1/10)#switchport mode trunk
Switch(Config-Ethernet1/10)#gvrp
Switch(Config-Ethernet1/10)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#gvrp
Switch(Config-Ethernet1/11)#exit
```

Switch C:

```
Switch(Config)#gvrp
Switch(Config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/2-6
Switch(Config-Vlan100)#exit
Switch(Config)#interface ethernet 1/11
Switch(Config-Ethernet1/11)#switchport mode trunk
Switch(Config-Ethernet1/11)#gvrp
Switch(Config-Ethernet1/11)#exit
```

9.4 VLAN Troubleshooting Help

9.4.1 Monitor and Debug Information

9.4.1.1 show vlan

Command: show vlan [brief| summary] [id <*vlan-id*>] [name <*vlan-name*>]

Function: Displays detailed information for all VLANs or a specified VLAN.

Parameters: brief stands for brief information; **summary** for VLAN statistics; **<*vlan-id*>** for VLAN ID of the VLAN to display status information, the valid range is 1 to 4094; **<*vlan-name*>** is the VLAN name for the VLAN to display status information, valid length is 1 to 11 characters.

Command mode: Admin Mode

Usage Guide: If no **<*vlan-id*>** or **<*vlan-name*>** is specified, then information for all VLANs in the switch will be displayed.

Example: Displaying the status for the current VLAN; displaying statistics for the current VLAN.

Switch#show vlan

VLAN	Name	Type	Media	Ports	
1	default	Static	ENET	Ethernet1/1	Ethernet1/2
				Ethernet1/3	Ethernet1/4
				Ethernet1/9	Ethernet1/10
				Ethernet1/11	Ethernet1/12
2	VLAN0002	Static	ENET	Ethernet1/5	Ethernet1/6
				Ethernet1/7	Ethernet1/8

Switch#sh vlan summary

The max. vlan entrys: 4094

Universal Vlan:

1 2

Total Existing Vlans is:2

Displayed information	Explanation
VLAN	VLAN number
Name	VLAN name
Type	VLAN property, of statically configured or dynamically learned.
Media	VLAN interface type: Ethernet
Ports	Access port within a VLAN

Universal Vlan	Universal VLAN.
Dynamic Vlan	Dynamic VLAN (not shown in this example)

9.4.1.2 show garp

Command: show garp [<*interface-name*>]

Function: Displays the global and port information for GARP.

Parameters: <*interface-nam*> stands for the name of the Trunk port to be displayed.

Command mode: Admin Mode

Usage Guide: N/A.

Example: Displaying global GARP information.

Switch #show garp

9.4.1.3 show gvrp

Command: show gvrp [<*interface-name*>]

Function: Displays the global and port information for GVRP.

Parameters: <*interface-nam*> stands for the name of the Trunk port to be displayed.

Command mode: Admin Mode

Usage Guide: N/A.

Example: Displaying global GVRP information.

Switch#show gvrp

---------- Gvrp Infomation ----------

Gvrp status : enable

Gvrp Timers(milliseconds)

LeaveAll : 10000

9.4.1.4 debug gvrp

Command: debug gvrp

no debug gvrp

Function: Enables the GVRP debug function: the "no debug gvrp**"** command disables this debugging function**.**

Command mode: Admin Mode

Default: GVRP debugging information is disabled by default.

Usage Guide: Use this command to enable GVRP debugging, GVRP packet processing information can be displayed.

Example: Enabling GVRP debug.

Switch#debug gvrp

9.4.2 VLAN Troubleshooting Help

☞ The GARP counter setting in for Trunk ports in both ends of Trunk link must be the same, otherwise GVRP will not work properly.

It is recommended to avoid enabling GVRP and RSTP at the same time in ES4704BD. If GVRP is to be enabled, RSTP function for the ports must be disabled first.

9.5 WEB MANAGEMENT

Click “Vlan configuration” to open the vlan allocation management list to manage the VLAN configuration of the switch.

9.5.1 Vlan configuration

Click “Vlan configuration”, “Vlan configuration” to open vlan allocation management list.

9.5.1.1 Create/remove Vlan

Click “Vlan configuration”, “Vlan configuration”, “Create/Remove VLAN” to open the adding/ deleting vlan management list of the switch .

9.5.1.1.1 VID allocation

Click “Vlan configuration”, “Vlan configuration”, “Create/Remove VLAN”, “VID allocation” to create and remove VLAN. Equals to CLI command 9.2.2.1:

- Operation type: Add new VID create a new means to VLAN; Remove means to remove a VLAN
- VID: specified VLAN ID

Example: Select “Add new VID” and set up VID as 100 and click Apply button then a new VLAN 100 is created.

VLAN ID information window will display current VLANs of the switch:

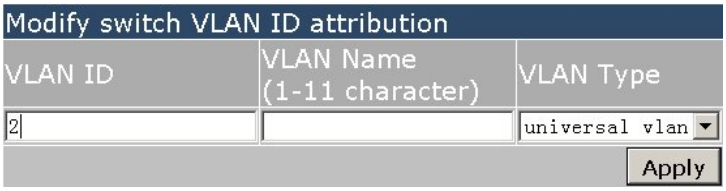
VLAN ID information		
VLAN ID	VLAN Name	VLAN Type
1	default	universal vlan
21	VLAN0021	universal vlan
41	VLAN0041	universal vlan
100	VLAN0100	universal vlan
124	VLAN0124	universal vlan

9.5.1.1.2 VID attribution configuration

Click “Vlan configuration”, “Vlan configuration”, “Create/Remove VLAN”, “VID attribution configuration” to setup VID type:

- VLAN ID: specified VLAN ID
- VLAN Name: allocate VLAN name. Equals to CLI command 9.2.2.2
- VLAN Type: VLAN type

Example: Set up VLAN ID as 2, VLAN Name as default and VLAN type as universal vlan and click Apply button then VLAN 2 is created.



VLAN ID information displays current VLAN allocation information of the switch:

VLAN ID information		
VLAN ID	VLAN Name	VLAN Type
1	default	universal vlan
2	2	universal vlan

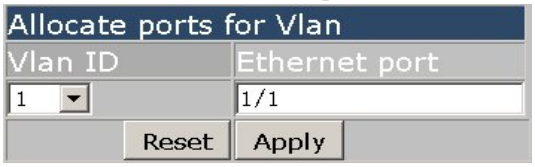
9.5.1.2 Allocate port for Vlan

Click “Vlan configuration”, “Vlan configuration”, Allocate ports for VLAN to open port VLAN allocation management list.

9.5.1.2.1 Allocate port for Vlan

Click “Vlan configuration”, “Vlan configuration”, Allocate ports for VLAN, Allocate port for Vlan to allocate ports for VLAN . Equals to CLI command 9.2.2.4

Select VLAN Num as 1, set port as 1/1 and click Apply button then port 1/1 will be added into 1/1.



Information display shows the VLAN allocation result:

9.5.1.3 Port type configuration

Click “Vlan configuration”, “Vlan configuration”, ”Port type configuration” to open port type configuration list.

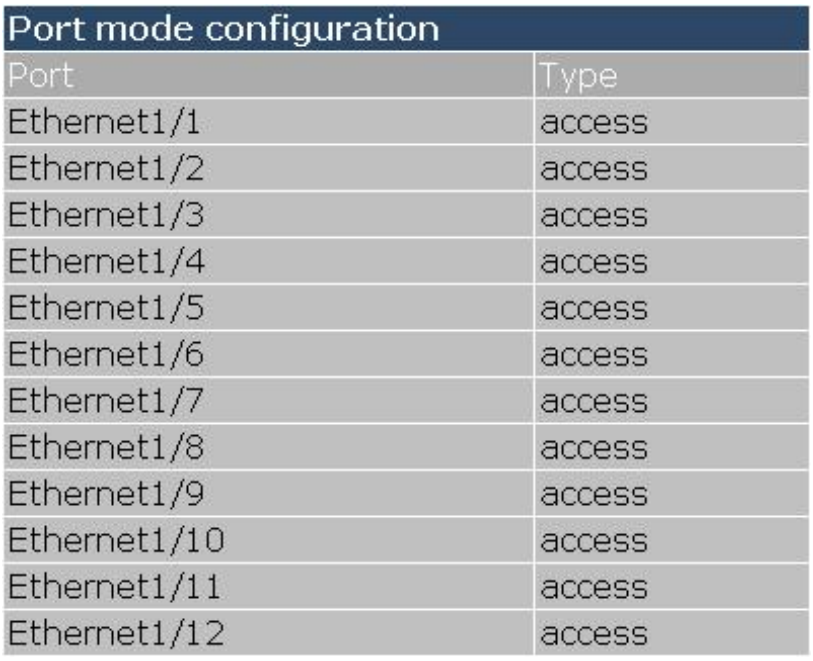
9.5.1.3.1 Set port mode(trunk/access)

Click “Vlan configuration”, “Vlan configuration”, “Port type configuration”, “Set port mode” (Trunk/Access) to set up port mode of the switch:

- Port: specified port
- Type: port mode including access mode and trunk mode. Equals to CLI command 9.2.2.5
- Vlan ingress rules: sets up open and close VLAN filter mode. Equals to CLI command 9.2.2.8

Example: Select Ethernet port 1/1, select port mode as Trunk and select Enable Vlan ingress rules and click the Apply button to apply this setting to the switch.

Port mode configuration to show port mode information



9.5.1.4 Trunk port configuration

Click “Vlan configuration”, “Vlan configuration”, “Trunk port configuration” to open Trunk port VLAN configuration list.

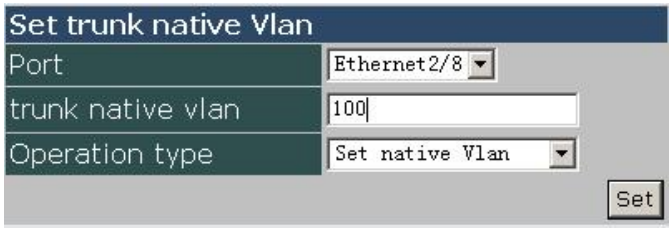
9.5.1.4.1 Vlan setting for trunk port

Click “Vlan configuration”, “Vlan configuration”, “Trunk port configuration”, “Vlan setting for trunk port” to set up trunk port VLAN type:

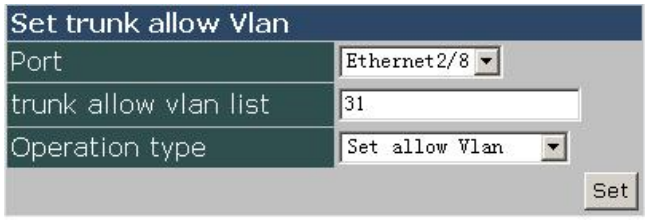
Set trunk native vlan. Equals to CLI command 9.2.2.7:

- Port: specifies port
- Trunk native vlan: specifies native vlan id
- Operation type: Sets native vlan means to add new VLAN; Remove native vlan means to remove original native vlan.

Example: Select port 2/8, set up Trunk native vlan as 100, select Operation type as Set native vlan and click the Set button so that the native vlan setting of port 2/8 will be vlan 100.



- Set trunk allow vlan. Equals to CLI command 9.2.2.6:
- Port: specified port
- Trunk allow vlan list: specifies allow vlan id list
- Operation type: Sets allow vlan means to add new allow VLAN; Remove allow vlan means to delete allow vlan



9.5.1.5 Set allow Vlan

Click “Vlan configuration”, “Vlan configuration”, “Access port configuration” to open Access port VLAN configuration list to allocate Access port VLAN.

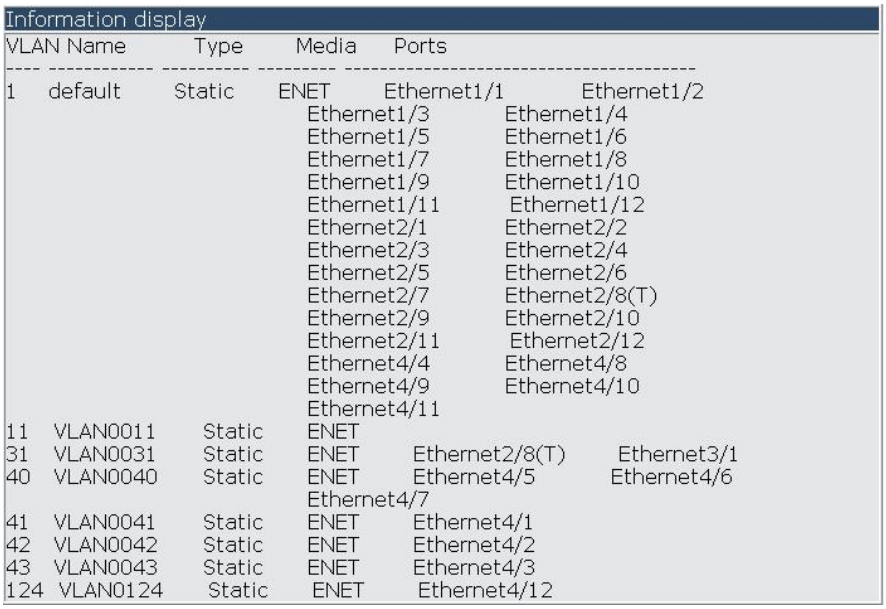
9.5.1.5.1 Vlan setting for access port

Click “Vlan configuration”, “Vlan configuration”, “Access port configuration”, “Vlan setting” to add current access ports to specified a VLAN or delete by VLAN:

- Port: specified port
- Vlan ID: Specified VLAN ID

Example: Select port Etherenet1/1, select VLAN ID 11 and click the Apply button then port 1/1 will be added into VLAN 11.

Information display will show current VLAN information of the switch:



9.5.1.6 Enable/Disable Vlan ingress rule

Click “Vlan configuration”, “Vlan configuration”, “Enable/Disable Vlan filter rule” to open VLAN ingress configuration list to setup VLAN filter function.

9.5.1.6.1 Disable Vlan ingress rule

Click “Vlan configuration”, “Vlan configuration”, to Enable/Disable Vlan ingress rule.

Example: Select Ethernet port 1/1 and click the Apply button and the VLAN ingress rule of port 1/1 will be disabled. Select Default button to enable the VLAN ingress rule.

9.5.2 GVRP configuration

Click “Vlan configuration”, “GVRP configuration” to open the GVRP configuration management list to manage GVRP function of the switch.

9.5.2.1 Enable global GVRP

Click “Vlan configuration”, “GVRP configuration”, “Enable global GVRP” to enable/disable the global GVRP function of the switch. Equals to CLI command 9.3.2.5.

Example: Select Enable GVRP and click Apply button to enable global GVRP function.

9.5.2.2 Enable port GVRP

Click “Vlan configuration”, “GVRP configuration”, to enable/disable port the GVRP function of the switch. Equals to CLI command 9.3.2.5.

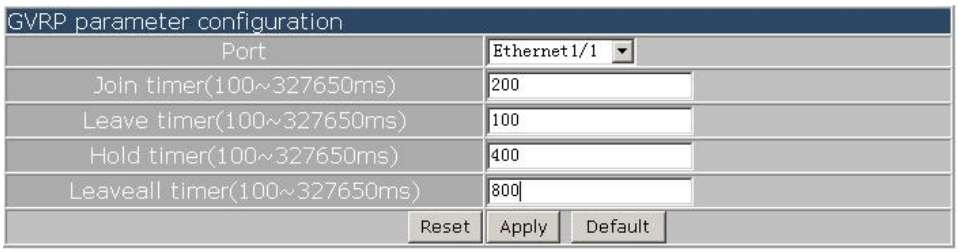
Example: Select Ethernet port 1/1, select Enable GVRP and click Apply button then the GVRP function of port 1/1 will be enabled. Note: only the Trunk port can enable GVRP function.

9.5.2.3 GVRP configuration

Click “Vlan configuration”, “GVRP configuration”, “GVRP configuration” to configure GVRP parameters of the switch：

- Port: specified port
- Join timer (100~327650ms): configures the value of GARP join timer. Equals to CLI command 9.3.2.1
- Leave timer (100~327650ms): configures the value of GARP leave timer. Equals to CLI command 9.3.2.2
- Hold timer (100~327650ms): configures the value of GARP hold timer. Equals to CLI command 9.2.3.3
- Leaveall timer (100~327650ms): configures the value of GARP leaveall timer. Equals to CLI command 9.2.3.4

Example: Select Ethernet port 1/1, setup Join timer as 200, Leave timers as 100, Hold timer as 400, Leaveall timer as 800. Click the Apply button to apply these settings to the switch.

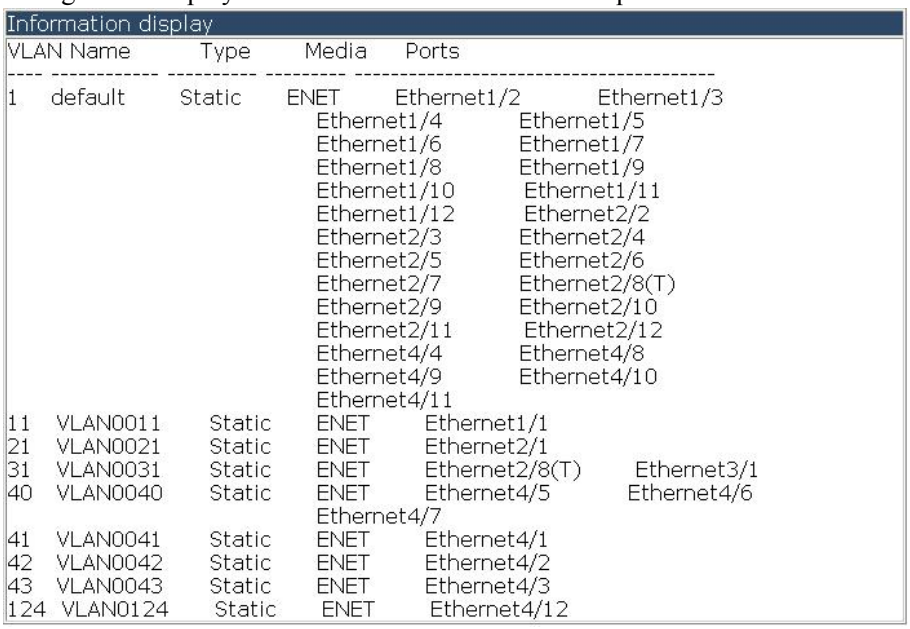


9.5.3 Vlan debug and maintenance

Click “Vlan configuration”, “Vlan debug” and “maintenance” to open VLAN debug management list to display related VLAN configuration information through the list.

9.5.3.1 Show vlan

Click “Vlan configuration”, “Vlan debug” and “maintenance”, “show Vlan” The display window in the right will display all related VLAN information. Equals to CLI command 9.4.1.1.



9.5.3.2 Show GARP

Click “Vlan configuration”, “Vlan debug” and “maintenance”, “show garp” The information window in the right will display all related GARP information. Equals to CLI command 9.4.1.2

9.5.3.3 Show GVRP

Click “Vlan configuration”, ”Vlan debug” and “maintenance”, “show gvrp”. The display window on the right will show all related GVRP information. Equals to CLI command 9.4.1.3

Information display
---------- Gvrp Infomation ----------
Gvrp status : enable
Gvrp Timers(milliseconds)
LeaveAll : 10000

Chapter 10 MSTP Configuration

10.1 Introduction to MSTP

MSTP is a new spanning tree protocol based on STP and RSTP. It runs on all bridges within a Bridged-LAN, calculating a simple connected tree active topology (CIST) for the Bridged-LAN (including bridges running MSTP, RSTP and STP), and calculating several separated multiple spanning tree instances (MSTI). It applies the fast converging properties, enabling multiple VLAN of the same topology to map to one spanning tree instance, while that spanning tree topology is independent of the other spanning tree instances. This mechanism provides an independent transmitting path for VLAN dataflow mapping to multiple spanning tree instances. On the other hand, several VLAN sharing one topology instance (MSTI) have substantial fewer spanning tree instances maintained by each bridge compared to the one-VLAN-one-spanning-tree implementation, therefore saving CPU resources and reducing non-communication bandwidth usage.

10.1.1 MSTP field

As Multiple VLANs can be mapped to a single Spanning Tree instance, the IEEE 802.1s counsel proposed the concept of MST field to workaround the determination of the VLAN-Spanning Tree Instance mapping issue.

A MSTP field consists of one or more bridges with identical MCIDs (MST Configuration Identification) and a LAN connecting all these bridges, where one bridge is a specified bridge of that LAN, with the bridges the LAN connects not running STP. All the bridges in the field maintain the same MSTIs.

Bridges in each field have the following properties:

- Configuration Name, consisting of alphanumeric characters.
- Configuration revision level.
- Configuration Digest of the VLAN in the bridges mapping to spanning tree instance.

The above three properties comprise the field MCID. Bridges are considered to belong to the same MST field only if they are identical in these three properties.

In the CIST of the whole Bridged-LAN, MSTP regard the MST as a bridge, as shown in the figure below:

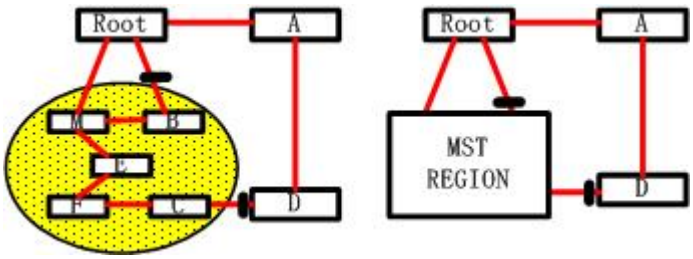


Fig 10-1 CIST and MST Field

As in the network in Fig 10-1, if the bridges in the network run STP or RSTP, then one of the ports between bridge M and bridge B should be blocked. However, if the bridges in the yellow part

of the figure run MSTP and are allocated in a MST field, then MSTP will treat that field as a single bridge and block the port between bridge B and Root; similarly, MSTP will block a port in network D.

10.1.1.1 MST field operation

All bridges in a field are connected via IST. When IST is running, CIST Regional Root will be elected as its root bridge, which has the lowest route cost to the CIST Root and smallest BridgeID. If only one field is present in the network, then that field becomes the CIST Root of the entire network; if the CIST Root falls outside the field, then a bridge at the field's edge will be elected to be the CIST Regional Root. The root port in the Field CIST Regional Root is Master Port to all the MSTI in the field.

When MSTP initializes, it will send a BPDU announcing itself as the CIST Regional Root and setting the route code to the CIST Root and CIST Regional Root to 0. The bridge will initialize all MSTIs at the same time it can claiming itself root of all MSTIs. If that bridge receives better CIST/MSTI root information (i.e., with lower route cost, BridgeId, etc), it will not continue as the root of CIST or corresponding MSTI.

Only IST sends and receives BPDUs in a field. BPDU convey information for all MSTI. As MST BPDUs carry information of all spanning tree instances, the BPDU number required to process the support of several spanning trees can be significantly reduced.

All instances in the MST field share a same protocol timer, but each instance has independent topology-specific parameters, such as Regional Root and root path costs, etc.

10.1.1.2 MST inter-field operation

When running multiple MST fields or IEEE 802.1D bridges (bridges running STP), MSTP maintains inter-field or field-802.1D bridges connections through CST. IST connects bridges in the field as a virtual bridges and connects to neighboring fields or 802.1D bridges.

The functional range of MSTI limits to the MST field it resides. Any MST instance in a field is independent of MST instances in other fields. When a bridge in the field receives a MST BPDU from another field, it will process only related CIST information in the data and discard MSTI information.

10.1.2 Port role

The MSTP bridge assigns a port role for each port running MSTP in accordance with each spanning tree.

- CIST port roles include: Root Port, Designated Port, Alternate Port and Backup Port.
- There is an additional role for MSTI ports besides the above-mentioned: Master Port.

The role assignment for Root Port, Designated Port, Alternate Port and Backup Port in CIST and each MSTI are similar to that of RSTP.

How does MSTP Load-balance Work?

When VLANs map to different spanning tree instances in a MST field, different topologies are created. All topology instances (including IST and MSTIs) are independent, and corresponding parameters (such as Bridge Priority, Port Cost) can be configured in the bridges. Assigning

corresponding roles to bridge and port can create routes corresponding to VLAN traffic in topology instances so as to achieve VLAN load balance. For detailed configurations, see the MSTP examples below.

10.2 MSTP Configuration

10.2.1 MSTP configuration task sequence

1. Enable MSTP and set the running mode
2. Configure instance parameters
3. Configure MSTP field parameter
4. Configure MSTP time parameter
5. Configure the fast migrate feature for MSTP

1. Enable MSTP and set the running mode

Command	Explanation
Global Mode and Port Mode.	
spanning-tree **no spanning-tree**	Enables/Disables MSTP
Global Mode	
spanning-tree mode {mstp|stp} **no spanning-tree mode**	Sets MSTP running mode
Port Mode	
spanning-tree mcheck	Forces port migration to run under MSTP

2. Configure instance parameters

Command	Explanation
Global Mode	
spanning-tree mst <*instance-id*> priority <*bridge-priority*> **no spanning-tree mst <*instance-id*> priority**	Sets bridge priority of the specified instance for the switch
Port Mode	
spanning-tree mst <*instance-id*> cost <*cost*> **no spanning-tree mst <*instance-id*> cost**	Sets the port route cost on a specified instance for the current port
spanning-tree mst <*instance-id*> port-priority <*port-priority*> **no spanning-tree mst <*instance-id*>**	Sets the port priority on a specified instance for the current port

port-priority	

3. Configure MSTP field parameters

Command	Explanation
Global Mode	
spanning-tree mst configuration **no spanning-tree mst configuration**	Enters MSTP field configuration mode; the **no spanning-tree mst configuration** command resets the MSTP field parameter to switch default.
MSTP field mode	
instance <*instance-id*> vlan <*vlan-list*> **no instance <*instance-id*> [vlan <*vlan-list*>]**	Creates a Instance and configures mapping between a VLAN and Instance.
name <*name*> **no name**	Sets the name for MSTP field.
revision-level <*level*> **no revision-level**	Sets the revision level for MSTP field.
abort	Exits MSTP field mode to Global mode without saving current configuration to MSTP field.
exit	Exits MSTP field mode to Global mode and saves current configuration to MSTP field.

4. Configure MSTP time parameters

Command	Explanation
Global Mode	
spanning-tree forward-time <*time*> **no spanning-tree forward-time**	Sets the value for the switch forward delay time
spanning-tree hello-time <*time*> **no spanning-tree hello-time**	Sets the Hello time of sending BPDU packets for the switch
spanning-tree maxage <*time*> **no spanning-tree maxage**	Sets the max age time for BPDU information in the switch
spanning-tree max-hop <*hop-count*> **no spanning-tree max-hop**	Sets the max hop count support for BPDU transmitting in MSTP field.

5. Configure the fast migrate feature for MSTP

Command	Explanation
Port Mode	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	Sets the port link type
spanning-tree portfast **no spanning-tree portfast**	Sets/Cancels setting for the port to be an edge port

10.2.2 Introduction to MSTP configuration commands

10.2.2.1 abort

Command: abort

Function: Discards the configuration in MSTP field and exits from MST mode to Global Mode.

Command mode: MSTP Field Mode.

Usage Guide: When using this command to exit MST mode, the configuration made to the MSTP field won't take effect and the previously saved MSTP field configuration remains effective. The "Ctrl+z" command is the keyboard equivalent to the "abort" command, i.e., exit without saving configuration changes.

Example: exiting MST mode without save the configuration changes.

Switch(Config-Mstp-Region)#abort

Switch(Config)#

10.2.2.2 exit

Command: exit

Function: Saves the configuration to MSTP field and exits from MSTP mode to Global Mode.

Command mode: MSTP Field Mode.

Usage Guide: when using this command exiting MST mode, changes made to MSTP field are applied at the same time.

Example: exiting MST mode and apply the configuration changes.

Switch(Config-Mstp-Region)#exit

Switch(Config)#

10.2.2.3 instance vlan

Command: instance <*instance-id*> vlan <*vlan-list*>

no instance <*instance-id*> [vlan <*vlan-list*>]

Function: creates an Instance and configures VLAN-instance mapping or adds VLAN table entries and specified instance mapping; the "no instance" removes a specified instance or mapping to specified instance.

Parameters: **<*instance-id*>** is the Instance number ranges from 0 to 48; **<*instance-id*>** is the Instance number from 1 to 48. **<*vlan-list*>** are non-consecutive VLAN number, supporting "-" symbol standing for the consecutive and nonsequence symbol ";".

Command mode: MSTP Field Mode.

Default: Before creating any instance, the switch has only Instance 0 and VLAN1 – 4094 all belong

to Instance 0.

Usage Guide: This command is used to set VLAN-Instance mapping. Switches are considered to be in the same MSTP field only if they have identical mapping and other MSTP field parameters. All VLANs belong to Instance 0 when no Instance has been configured. MSTP support up to 48 MSTI (excluding CIST). CIST can be considered to be MSTI 0, while the rest of the instances be MSTI 1 to 48. Detailed number is determined by specific product specification, 48 is the maximal value for the specification.

Example: Configuring the mapping between VLAN1-10;100-110 and Instance 1

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1-10;100-110

10.2.2.4 name

Command: name <*name*>

no name

Function: Configures the MSTP field name in MSTP Field mode; the "no name" command deletes the MSTP field name.

Parameters: <*name*> is the MSTP field name, which can be a string of 32 bytes or less.

Command mode: MSTP Field Mode.

Default: The default MSTP field name is the Switch bridge MAC.

Usage Guide: This command is used to set the MSTP field name. Switches are considered to be in the same MSTP field only if they have identical MSTP field names and other MSTP field parameters.

Example: Setting the MSTP field name to "mstp-test".

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#name mstp-test

10.2.2.5 revision-level

Command: revision-level <*level*>

no revision-level

Function: Configures the revision level for calculation MST configuration ID in MST mode; the "no revision-level" reverts the revision level to its default value 0.

Parameters: < *level*> is the revision level ranging from 0 to 65535.

Command mode: MSTP Field Mode.

Default: The default revision level is 0.

Usage Guide: This command is used to set the revision level that is used in calculation MST configuration ID. Switches are considered to be in the same MSTP field only if they have identical revision levels and other MSTP field parameters.

Example: Setting the revision level to 2000.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)# revision-level 2000

10.2.2.6 spanning-tree

Command: spanning-tree

no spanning-tree

Function: Enables MSTP in Global Mode and Port Mode; the "**no spanning-tree**" command disables MSTP.

Command mode: Global Mode and Port Mode

Default: MSTP is disabled by default.

Usage Guide: If MSTP is enabled in Global mode, MSTP will be enabled on all ports except those already running applications mutually exclusive to MSTP.

Example: Enabling MSTP under Global Mode and disabling MSTP for port 1/2.

Switch(Config)#spanning-tree

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#no spanning-tree

10.2.2.7 spanning-tree forward-time

Command: spanning-tree forward-time <*time*>

no spanning-tree forward-time

Function: Sets the delay time before forwarding; the "**no spanning-tree forward-time**" command restores the default setting.

Parameters: < *time*> is the forward delay time in seconds , the valid range is 4 to 30.

Command mode: Global Mode

Default: The default forward delay time is 15 seconds.

Usage Guide: When the network topology changes, the delay time for a port changes from blocking status to listening status. This is called forward delay time. The forward delay time, Hello time and max age time are associated. When configuring MSTP time parameters, the following conditions must be met, otherwise the MSTP may not work properly:

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

Example: Setting MSTP forward delay time to 20 seconds in Global Mode.

Switch(Config)#spanning-tree forward-time 20

10.2.2.8 spanning-tree hello-time

Command: spanning-tree hello-time <*time*>

no spanning-tree hello-time

Function: Sets the Hello time for the switch; the "**no spanning-tree hello-time**" command restores the default setting.

Parameters: < *time*> is the Hello time in seconds, the valid range is 1 to 10.

Command mode: Global Mode

Default: The default Hello time is 2 seconds.

Usage Guide: The interval for switch to send a BPDU is referred to as Hello time. The Hello time, forward delay time, and max age time are associated. When configuring these time parameters, the following conditions must be met, otherwise the MSTP may not work properly.

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

Example: Setting MSTP Hello time to 5 seconds in Global Mode.

Switch(Config)#spanning-tree hello-time 5

10.2.2.9 spanning-tree link-type p2p

Command: spanning-tree link-type p2p {auto|force-true|force-false}

no spanning-tree link-type

Function: Sets the link types connected to the current port; the "**no spanning-tree link-type**" command restores the link type to auto-detect.

Parameters: auto stands for auto-detection of link type; **force-true** stands for forced point-to-point; **force-false** stands for forced non-point-to-point.

Command mode: Port configuration Mode

Default: MSTP auto-detects the link type connected to the port by default.

Usage Guide: When the port is operating under full-duplex mode, MSTP will assume the link connected to the port to be point-to-point type; while under half-duplex mode, MSTP assumes the link connected to be shared type

Example: Setting the link of port 1/7-8 to be forced point-to-point type.

Switch(Config)#interface ethernet 1/7-8

Switch(Config-Port-Range)#spanning-tree link-type p2p force-true

10.2.2.10 spanning-tree maxage

Command: spanning-tree maxage <*time*>

no spanning-tree maxage

Function: Sets the maximum age time for the switch's BPDU messages; the "**no spanning-tree maxage**" command restores the default setting.

Parameters: < *time*> is the max. age time in seconds , ranging from 6 to 40.

Command mode: Global Mode

Default: The default maximum age time is 20 seconds.

Usage Guide: The lifecycle for BPDU is referred to as the max age time. The max age time, forward delay time, and Hello time are associated. When configuring MSTP time parameters, the following conditions must be met, otherwise the MSTP may not work properly.

2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)

Example: Setting the maximum age time to 25 seconds in Global Mode.

Switch(Config)#spanning-tree maxage 25

10.2.2.11 spanning-tree max-hop

Command: spanning-tree max-hop <*hop-count*>

no spanning-tree max-hop

Function: Sets the maximum hops allowed for connecting to the port; the "**no spanning-tree max-hop**" command restores the default settings.

Parameters: < *hop-count*> is the max hop count, the valid range is 1 to 40.

Command mode: Global Mode

Default: The default maximum is 20 hops.

Usage Guide: MSTP not only keeps Max-age for BPDU lifecycle, but a Max-hop added to the MSTP field standing for BPDU lifecycle. The max-hop count decreases when packets transmit through the network. A BPDU message reaches its max Max-hop upon leaving the root bridge of MSTI, each time BPDU is received, the Max-hop value decrements by 1. When a port receives a BPDU with Max-hop 0, it will drop that BPDU and make itself the designated port for sending BDPUs.

Example: Setting the max-hop count to 32.

Switch(Config)#spanning-tree max-hop 32

10.2.2.12 spanning-tree mcheck

Command: spanning-tree mcheck

Function: Forces port migration to run under MSTP.

Command mode: Port configuration Mode

Default: Ports are operating under MSTP by default.

Usage Guide: If bridges running IEEE 802.1D STP exist in the segment connected to the current Ethernet port, this port will migrate to the STP compatible mode. When the network is fairly stable, even if the bridge running STP is disconnected, the associated port running MSTP will continue running in STP compatible mode, and this command can be used to force the port to migrate to MSTP mode. When the port migrates to MSTP, it will switch back to STP compatible mode on receiving news STP packets,

This command can only be executed when the switch is running in IEEE 802.1s MSTP mode, and will be invalid if the switch is configured in IEEE 802.1D STP mode.

Example: Forcing port 1/2 migrate MSTP mode.

Switch(Config-Ethernet1/2)#spanning-tree mcheck

10.2.2.13 spanning-tree mode

Command: spanning-tree mode {mstp|stp}

no spanning-tree mode

Function: Sets the switch to run in Spanning Tree mode; the "**no spanning-tree mode**" command restores the default setting.

Parameters: mstp sets the switch in IEEE 802.1s MSTP mode; **stp** sets the switch in IEEE 802.1D STP mode.

Command mode: Global Mode

Default: The switch runs in MSTP by default.

Usage Guide: When the switch is running in IEEE 802.1D STP, only standard 802.1D BPDU frames and TCN BPDU frames can be sent, any MSTP BPDU frames received will be dropped.

Example: Setting the switch to STP mode.

Switch(Config)#spanning-tree mode stp

10.2.2.14 spanning-tree mst configuration

Command: spanning-tree mst configuration

no spanning-tree mst configuration

Function: Enter the MST configuration mode of the switch, in MST configuration mode of the switch, switch specific MSTP field parameter can be configured; the "**no spanning-tree mst configuration**" command resets the default switch MSTP field parameter.

Command mode: Global Mode

Default: The default MSTP field parameters, before the user enters MST configuration mode, are shown below:

MSTP Field Parameter	Parameter default
Instance	Only Instance 0 exists, and VLAN1 – 4094 all map to instance 0.
Name	Take the Switch bridge MAC.
Revision	0

Usage Guide: Whether MSTP is enabled on the switch, you can always enter the MSTP field configuration mode and save your changes after configuration. When the switch is running in MSTP mode, the system will calculate the MST configuration Identifier (ID) according to the MSTP field parameters configured, only switches with identical MSTP field configuration Identifiers will be considered to be in the same MSTP field, and allow MSTI calculation.

Example: Entering the MST configuration mode for the switch.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#

10.2.2.15 spanning-tree mst cost

Command: spanning-tree mst <*instance-id*> cost <*cost*>

no spanning-tree mst <instance-id> cost

Function: Sets the route cost for the current Ethernet port; "**no spanning-tree mst <instance-id> cost**" command restores the default value.

Parameters: <*instance-id*> is the instance ID of the specified instance, ranging from 0 – 48; **<*cost*>** is the route cost value, ranging from 1 - 200,000,000.

Command mode: Port configuration Mode

Default: The route cost for the port corresponds to the port bandwidth by default.

Port Type	Default route cost	Recommended Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000
10Gbps	2000	2000~20000

For the port channel, the default port route cost is shown below:

Port Type	Aggregated port number (inside allowed aggregating number).	Default route cost
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N
10Gbps	N	2000/N

Usage Guide: Sets the route cost for the ports that can control the rout routing cost from the instance port to the root bridge, so as to control the election of root port and designated ports.

Example: Setting the port 1/2 route cost of the MSTP port corresponding to Instance 2 to 3000000.

Switch(Config-Ethernet1/2)#spanning-tree mst 2 cost 3000000

10.2.2.16 spanning-tree mst port-priority

Command: spanning-tree mst <*instance-id*> port-priority <*port-priority*>

no spanning-tree mst <*instance-id*> port-priority

Function: Sets the priority of the current port on the specified instance; the "**no spanning-tree mst**" command restores the default port priority value.

Parameters: <*instance-id*> is the instance ID of the designated instance ranging from 0 – 48; valid **<*port-priority*>** is the port priority value, which is multiples of 16 between 0 to 240, i.e., 0, 16, 32, 48,…, 240.

Command mode: Port configuration Mode

Default: The default port priority value is 128.

Usage Guide: Port ID of the designated instance can be configured by setting port priority, further effecting the root port and designated port election. A smaller port priority value means higher

priority.

Example: Setting the priority for port 1/2 of instance1 to 32.

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#spanning-tree mst 1 port-priority 32

10.2.2.17 spanning-tree mst priority

Command: spanning-tree mst <*instance-id*> priority <*bridge-priority*>

no spanning-tree mst <*instance-id*> priority

Function: Sets the switch bridge priority of the specified instance; the "**no spanning-tree mst**" restores the default priority value for the switch on the specified instance.

Parameters: **<*instance-id*>** is the instance ID of the designated instance ranging from 0 – 48; **<*port-priority*>** is the port priority value, which is multiples of 4096 between 0 to 61440, i.e., 0, 4096, 8192,… 61440.

Command mode: Global Mode

Default: The default switch priority is 32768.

Usage Guide: Bridge ID of the specified instance can be changed by setting switch priority, therefore affecting the root bridge and designated port election for that instance. A smaller switch bridge priority value means a higher priority.

Example: The default switch instance2 priority is 4096.

Switch(Config)#spanning-tree mst 2 priority 4096

10.2.2.18 spanning-tree portfast

Command: spanning-tree portfast

no spanning-tree portfast

Function: Sets the current port as an edge port; the "**no spanning-tree portfast**" command sets the current port as a non-edge port.

Command mode: Port configuration Mode

Default: All ports are non-edge ports on initial MSTP start.

Usage Guide: When a port is configured as an edge port, it can switch from Discarding status to Forwarding status instantly without the forward delay. Once BPDU frames are received on an edge port, the port changes to a non-edge port automatically.

Example: Configuring port 1/5-6 to be edge ports.

Switch(Config)#interface ethernet 15-6

Switch(Config-Port-Range)#spanning-tree portfast

10.3 MSTP Example

The following is a typical MSTP application scenario:

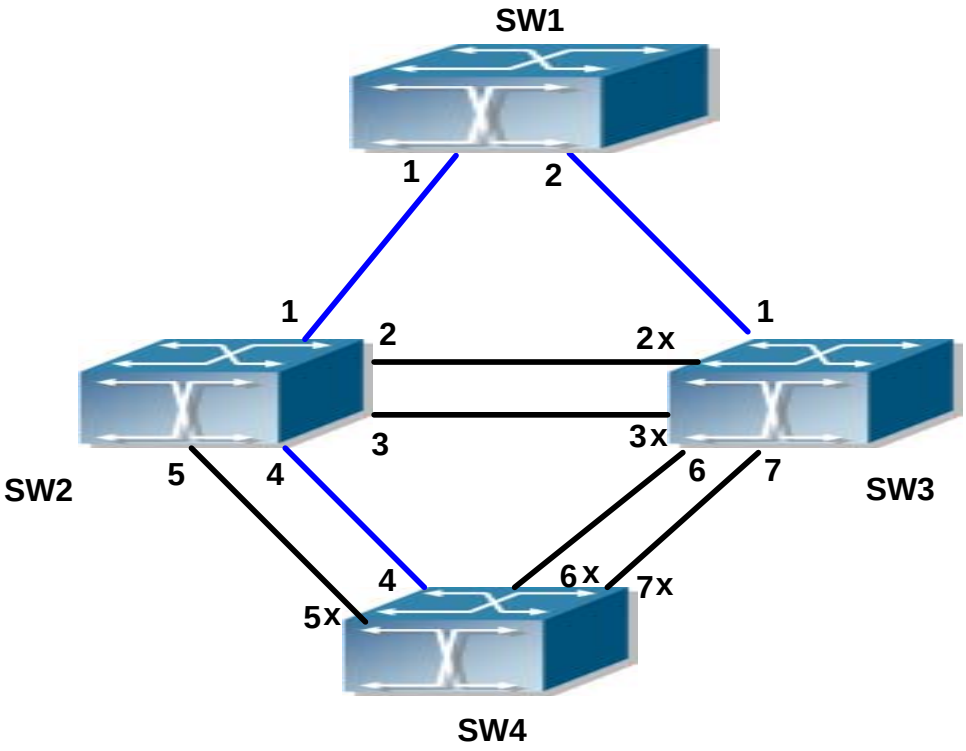


Figure 10-2 MSTP Typical Application Example

As illustrated in the figure above by the lines between SW1-SW4, MSTP is running. All the switches run in MSTP mode by default, their bridge priority, port priority and port route cost are all the default values (equal). The default configuration for switches are listed below:

Bridge name		SW1	SW2	SW3	SW4
Bridge MAC address		…00-00-01	…00-00-02	…00-00-03	…00-00-04
Bridge Priority		32768	32768	32768	32768
Port Priority	Port 1	128	128	128	
	Port 2	128	128	128	
	Port 3		128	128	
	Port 4		128		128
	Port 5		128		128
	Port 6			128	128
	Port 7			128	128
Port route	Port 1	200000	200000	200000	
	Port 2	200000	200000	200000	
	Port 3		200000	200000	

	Port 4		200000		200000
	Port 5		200000		200000
	Port 6			200000	200000
	Port 7			200000	200000

By default, MSTP will establish a topology (in blue lines) rooted with SW1, the ports marked with “x” are in the Discarding status, the other ports are in the Forwarding status.

Configurations adjustment:

Step 1: Configure port-VLAN mapping.

- Create VLAN 20, 30, 40, 50 in Switch SW2, SW3, and SW4.
- Set the port 1-7 to Trunk mode in Switch SW2, SW3, and SW4.

Step 2: Configure Switch SW2, SW3, SW4 to be in the same MSTP field.

- Configure the filed name for SW2, SW3, SW4 to "mstp";
- Map vlan 20 and vlan 30 on SW2, SW3 and SW4 to Instance3; map vlan 40 and vlan 50 to Instance4.

Step 3: Configure switch SW3 to be the root bridge of Instance3; Configure switch SW4 to be root bridge of Instance4.

- Set in Switch SW3 the corresponding bridge priority of Instance3 to 0;
- Set in Switch SW4 the corresponding bridge priority of Instance4 to 0.

The configuration steps are listed below:

Switch SW2:

SW2(Config)#vlan 20

SW2(Config-Vlan20)#exit

SW2(Config)#vlan 30

SW2(Config-Vlan30)#exit

SW2(Config)#vlan 40

SW2(Config-Vlan40)#exit

SW2(Config)#vlan 50

SW2(Config-Vlan50)#exit

SW2(Config)#spanning-tree mst configuration

SW2(Config-Mstp-Region)#name mstp

SW2(Config-Mstp-Region)#instance 3 vlan 20;30

SW2(Config-Mstp-Region)#instance 4 vlan 40;50

SW2(Config-Mstp-Region)#exit

SW2(Config)#interface e1/1-7

SW2(Config-Port-Range)#switchport mode trunk

SW2(Config-Port-Range)#exit

SW2(Config)#spanning-tree

Switch SW3:

SW3(Config)#vlan 20
SW3(Config-Vlan20)#exit
SW3(Config)#vlan 30
SW3(Config-Vlan30)#exit
SW3(Config)#vlan 40
SW3(Config-Vlan40)#exit
SW3(Config)#vlan 50
SW3(Config-Vlan50)#exit
SW3(Config)#spanning-tree mst configuration
SW3(Config-Mstp-Region)#name mstp
SW3(Config-Mstp-Region)#instance 3 vlan 20;30
SW3(Config-Mstp-Region)#instance 4 vlan 40;50
SW3(Config-Mstp-Region)#exit
SW3(Config)#interface e1/1-7
SW3(Config-Port-Range)#switchport mode trunk
SW3(Config-Port-Range)#exit
SW3(Config)#spanning-tree
SW3(Config)#spanning-tree mst 3 priority 0

Switch SW4:

SW4(Config)#vlan 20
SW4(Config-Vlan20)#exit
SW4(Config)#vlan 30
SW4(Config-Vlan30)#exit
SW4(Config)#vlan 40
SW4(Config-Vlan40)#exit
SW4(Config)#vlan 50
SW4(Config-Vlan50)#exit
SW4(Config)#spanning-tree mst configuration
SW4(Config-Mstp-Region)#name mstp
SW4(Config-Mstp-Region)#instance 3 vlan 20;30
SW4(Config-Mstp-Region)#instance 4 vlan 40;50
SW4(Config-Mstp-Region)#exit
SW4(Config)#interface e1/1-7
SW4(Config-Port-Range)#switchport mode trunk

SW4(Config-Port-Range)#exit

SW4(Config)#spanning-tree

SW4(Config)#spanning-tree mst 4 priority 0

After the above configuration, all instance CIST (Instance0) of the entire network take SW1 as the root bridge, and in the MSTP fields in which SW2, SW3 and SW4 reside, the region root of Instance0 is SW2, and SW3 for Instance3, SW4 for Instance4. The traffic of vlan 20 and vlan 30 transmit along the topology of Instance3; traffic of vlan 40 and vlan 50 transmit along the topology of Instance4; traffic of other vlan transmit along topology of Instance0. Port 1 of Switch SW2 is the Master Port of Instance3 and Instance4.

MSTP calculation results include three topologies Instance0, Instance3 and Instance4, as shown in the figure below (indicated with blue lines). Ports with "x" are in "Discarding" mode and the other ports are in "Forwarding" mode. Since Instance3 and Instance4 are valid only in MSTP field, only topology in the MSTP field for the related parts are shown in the figure.

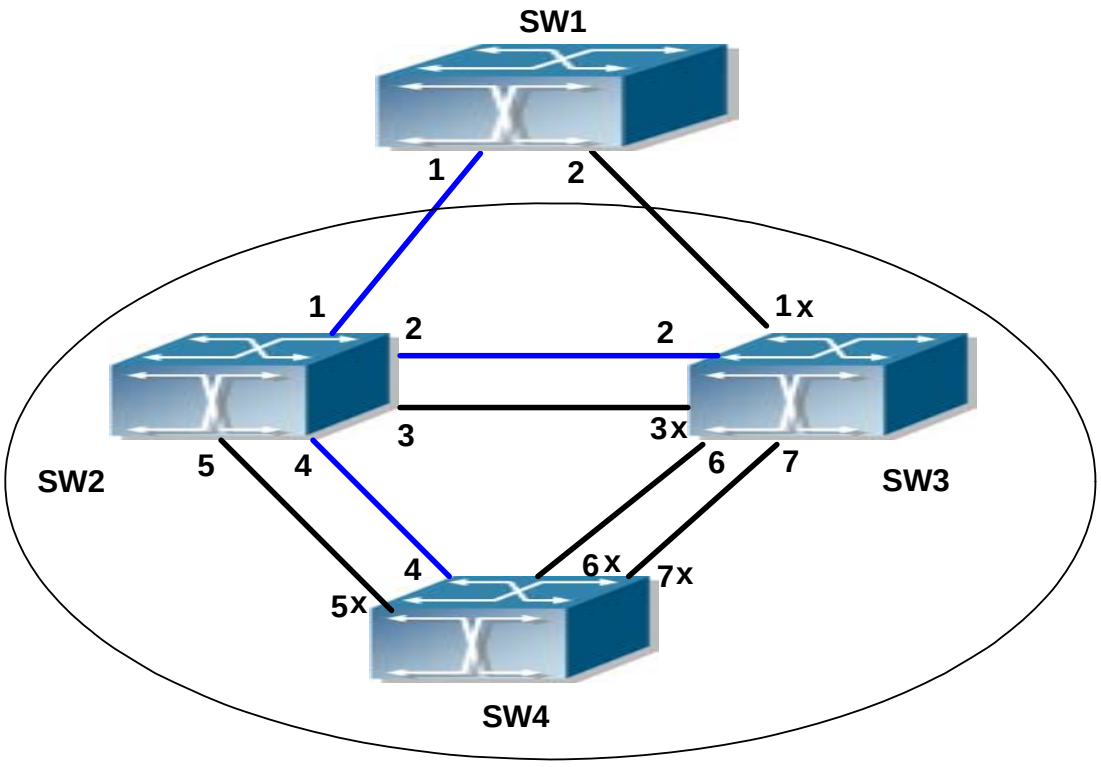


Figure 10-3 Instance0 topology after MSTP change

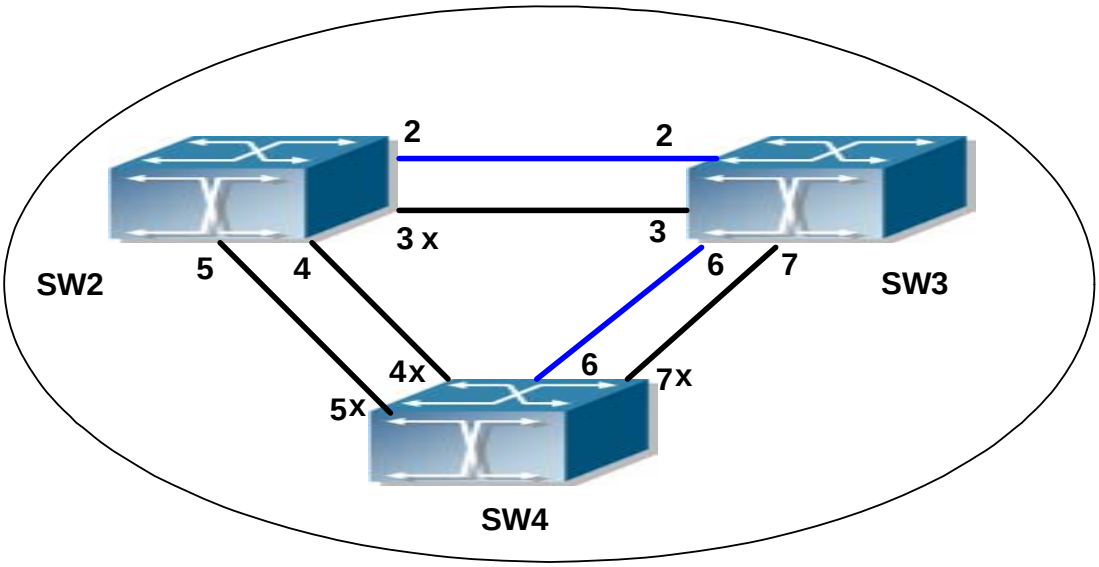


Figure 10-4 Instance3 topology in the MSTP field after MSTP change

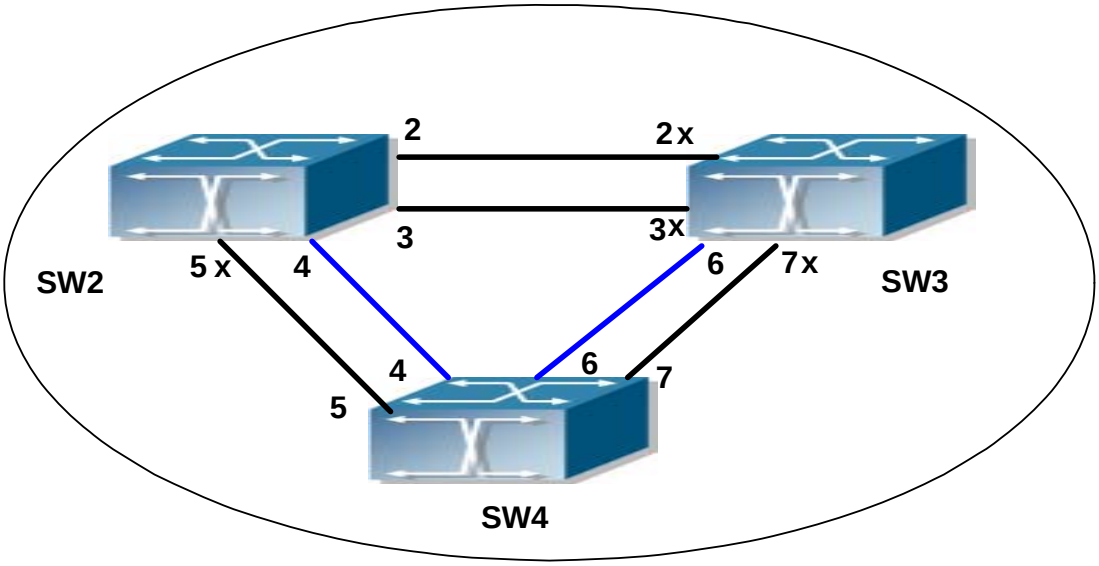


Figure 10-5 Instance4 topology in the MSTP field after MSTP change

10.4 MSTP Troubleshooting Help

10.4.1 Monitor and Debug Command

10.4.1.1 show spanning-tree

Command: show spanning-tree [mst [<*instance-id*>]] [interface <*interface-list*>] [detail]

Function: Displays MSTP and instances information.

Parameters: <***interface-list***> is the port list; <***instance-id***> is the instance value ranging from 0 to 48; <***interface-list***> is the port list; **detail** stands for display detailed spanning-tree information.

Command mode: Admin Mode

Usage Guide: The bridge and instance MSTP information, field configuration information and port

MSTP information can be displayed with the “show spanning-tree” command.

Example: Displaying MSTP information, the displayed contents are shown below.

```
Switch#sh spanning-tree

                    -- MSTP Bridge Config Info --

Standard        :   IEEE 802.1s
Bridge MAC      :   00:03:0f:01:0e:30
Bridge Times :   Max Age 20, Hello Time 2, Forward Delay 15
Force Version:   3

############################## Instance 0 ##############################
Self Bridge Id     : 32768 -   00:03:0f:01:0e:30
Root Id                : 16384.00:03:0f:01:0f:52
Ext.RootPathCost : 200000
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID       : 128.1
Current port list in Instance 0:
Ethernet1/1 Ethernet1/2 (Total 2)

 PortName          ID          ExtRPC     IntRPC    State Role        DsgBridge        DsgPort
-------------- ------- --------- --------- --- ---- ------------------ -------
 Ethernet1/1    128.001             0             0 FWD ROOT 16384.00030f010f52 128.007
 Ethernet1/2    128.002             0             0 BLK ALTR 16384.00030f010f52 128.011

############################## Instance 3 ##############################
Self Bridge Id     : 0.00:03:0f:01:0e:30
Region Root Id     : this switch
Int.RootPathCost : 0
Root Port ID       : 0
Current port list in Instance 3:
Ethernet1/1 Ethernet1/2 (Total 2)

  PortName          ID       IntRPC     State Role        DsgBridge        DsgPort
-------------- ------- --------- --- ---- ------------------ -------
 Ethernet1/1    128.001             0 FWD MSTR         0.00030f010e30 128.001
 Ethernet1/2    128.002             0 BLK ALTR         0.00030f010e30 128.002
```

############################## Instance 4 ##############################

Self Bridge Id : 32768.00:03:0f:01:0e:30

Region Root Id : this switch

Int.RootPathCost : 0

Root Port ID : 0

Current port list in Instance 4:

Ethernet1/1 Ethernet1/2 (Total 2)

PortName	ID	IntRPC	State	Role	DsgBridge	DsgPort
Ethernet1/1	128.001	0	FWD	MSTR	32768.00030f010e30	128.001
Ethernet1/2	128.002	0	BLK	ALTR	32768.00030f010e30	128.002

Displayed information	Explanation
Bridge information.	
Standard	STP version
Bridge MAC	MAC of the current bridge.
Bridge Times	The configured value for Max Age, Hello Time and Forward Delay of the current bridge.
Force Version	Version value of the current running STP.
Instance Information	
Self Bridge Id	Priority and MAC of the current bridge corresponding to the Instance.
Root Id	Priority and MAC of the root bridge corresponding to the Instance.
Ext.RootPathCost	Path cost of the bridge to the master root of the entire network.
Int.RootPathCost	Path cost of the bridge to the instance field root.
Root Port ID	Root port of the instance in the bridge.
Effective MSTP port list in the instance	
PortName	Port name
ID	Port priority and port index value
ExtRPC	Path cost of the port to the master root of the entire network.
IntRPC	Path cost of the port to the instance field root.
State	Port status for the instance
Role	Port role for the instance
DsgBridge	Upstream designated bridge for the instance port
DsgPort	Upstream designated port for the instance port

10.4.1.2 show mst configuration

Command: show spanning-tree mst config

Function: Displays the effective MSTP field parameter configurations in admin mode.

Command mode: Admin Mode

Usage Guide: The command displays the current effective parameter of the MSTP field, such as MSTP field name, revision level, VLAN-instance mapping, etc.

Example: Displaying the MSTP field configuration for the switch.

Switch#show spanning-tree mst config

```
Name        edgecore
Revision    0
Instance    Vlans Mapped
----------------------------------
00          1-29, 31-39, 41-4094
03          30
04          40
```

10.4.1.3 show mst-pending

Command: show mst-pending

Function: Displays effective MSTP field parameter configurations in MSTP field mode.

Command mode: MSTP Field Mode.

Usage Guide: enter this command to display the current parameter of the MSTP field, such as MSTP field name, revision level, VLAN-instance mapping, etc.

Note: The displayed parameter configuration may have not take effect until exiting the MSTP Field Mode.

Example: Displaying the current MSTP Field configuration for the switch.

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#show mst-pending

```
Name        edgecore
Revision    0
Instance    Vlans Mapped
----------------------------------
00          1-29, 31-39, 41-4093
03          30
04          40
05          4094
----------------------------------
```

Switch(Config-Mstp-Region)#

10.4.1.4 debug spanning-tree

Command: debug spanning-tree

no debug spanning-tree

Function: Enables MSTP debug information: the "**no debug spanning-tree"** command disables MSTP debug information**.**

Command mode: Admin Mode

Usage Guide: This command is the main switch for the sophisticated MSTP debugging functions, turn on the debugging information as needed in each level, then turn on the main switch to enable debugging information printouts. Debug switch in all the levels including: view MSTP running BPDU packet sending/receiving, events handling, status machine, counters, etc. The debugging information is typically used for adjustments by technicians; users can ignore such information.

Example: Enabling the debug information for receiving BPDU packets on port 1/1.

Switch#debug spanning-tree

Switch#debug spanning-tree bpdu rx interface e1/1

10.4.2 MSTP Troubleshooting Help

- If MSTP is to be run in the switch, MSTP must be first enabled globally. Before enabling global MSTP, port MSTP must not allowed be enabled.
- MSTP timer parameters are related, improper configuration may render the switch unable to work properly. The relationship between the timers are:

  2×(Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
- When modifying MSTP parameters, the user should be aware of the resulting topology. All parameter configurations, except those bridge based global settings, are instance-based configurations, caution should be taken to ensure parameter-instance agreement during configuration.
- The MSTP function, port MAC binding and 802.1x function of ES4704BD are mutually exclusive. When MAC binding and IEEE 802.1x are configured, MSTP cannot be enabled.

10.5 WEB MANAGEMENT

Click “MSTP control” to enter MSTP control configuration mode to manage MSTP features for the switch.

10.5.1 MSTP field operation

Click “MSTP control” to enter MSTP field operation.

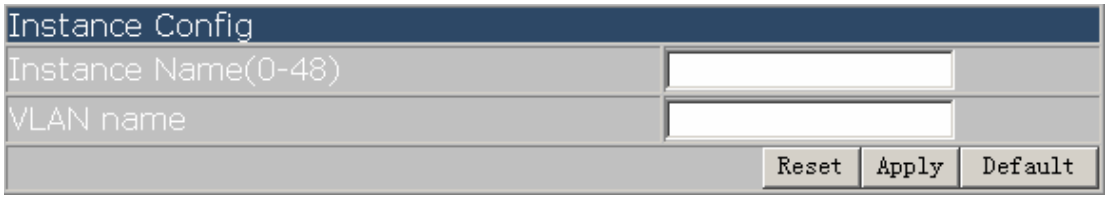
10.5.1.1 Instance configuration

Click “MSTP control” to enter MSTP field operation, then Instance configuration.

Create the Instance and configure the VLAN-Instance mapping or add VLAN table entry mapping to specified Instance.

Configure mapping between VLAN1-10;100-110 and Instance 1. Equivalent command 1.2.1.3.

Set Instance name to 1, VLAN name to VLAN1-10;100-110. Click "Apply" to commit the application.

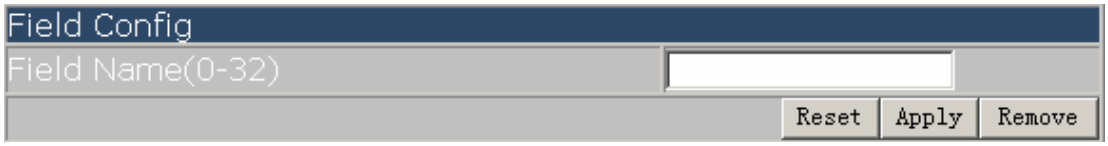


10.5.1.2 Field operation

Click “MSTP control” to enter the MSTP field operation.

Configure MSTP field name under MSTSP field configuration mode.

Set the MSTP field name to "mstp-test". Equivalent command 1.2.1.4.

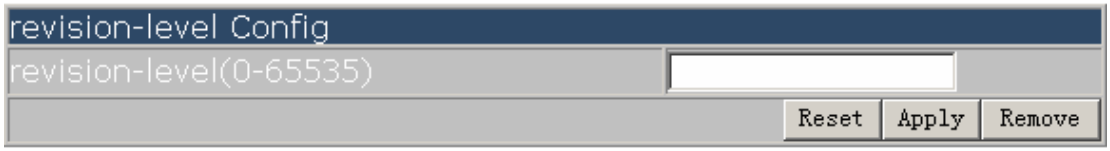


10.5.1.3 Revision level control

Click “MSTP control” to enter MSTP field operation, then "revision-level Config".

Configure the revision level value for calculating MST configuration ID under MST configuration mode.

Set the revision level to 2000.



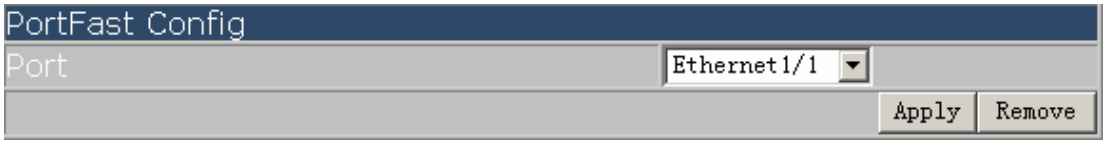
10.5.2 MSTP port operation

10.5.2.1 Edge port setting

Click “MSTP control” to enter MSTP field operation, then "PortFast Config".

Set the port to be an edge port

Configure port 1/5 to be edge ports.

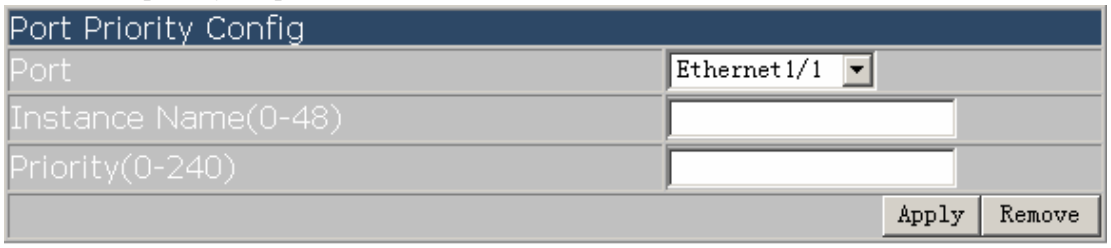


10.5.2.2 Port priority setting

Click “MSTP control” to enter MSTP port operation, then "Port Priority Config".

Set the priority for the current port on specified instance

Set the priority for port 1/2 of instance1 to 32.

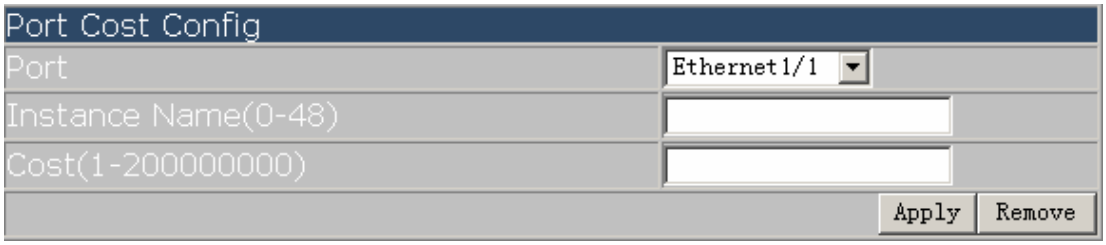


10.5.2.3 Port route cost setting

Click “MSTP control” to enter MSTP port operation, then "Port Cost Config".

Set the port route cost on specified instance for the current port

Set on port 1/2 route cost of the MSTP port corresponding to Instance 2 to 3000000.

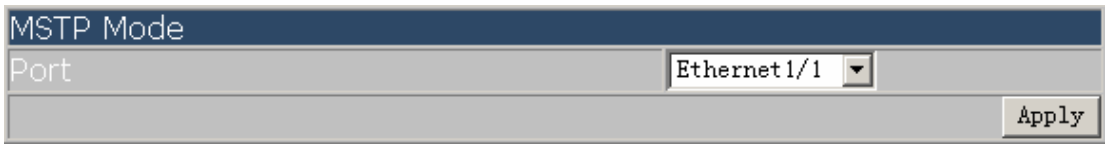


10.5.2.4 MSTP mode

Click “MSTP control” to enter MSTP port operation, then "MSTP Mode".

Force switch port migrate to run under MSTP.

Force port 1/2 migrate to run under MSTP.

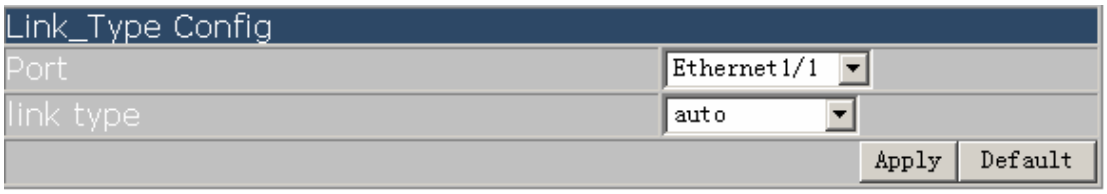


10.5.2.5 Link type configuration

Click “MSTP control” to enter MSTP port operation, then "Link_Type Config".

Set the link type of the current port.

Set the link of port 1/7 to be forced point-to-point type.

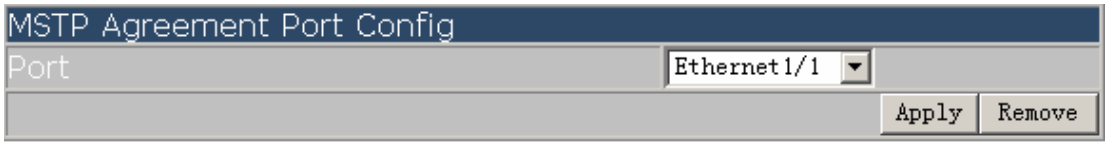


10.5.2.6 MSTP port configuration

Click “MSTP control” to enter MSTP port operation, then "MSTP Agreement Port Config".

Run the command to enable MSTP under the switch port configuration mode.

Enable MSTP under Global Mode and disable MSTP for port 1/2.



10.5.3 MSTP global control

10.5.3.1 MSTP global protocol port configuration

Click “MSTP control” to enter MSTP Global control, then "MSTP Global Agreement Port Config".

Run MSTP enable command under the switch port configuration mode.

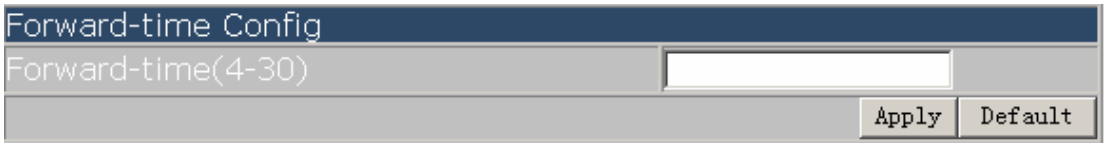
Enable MSTP in Global mode.

10.5.3.2 Forward delay time configuration

Click “MSTP control” to enter MSTP Global control, then "Forward-time Config".

Set the value for switch forward delay time

Set MSTP forward delay time to 20 seconds in Global Mode.

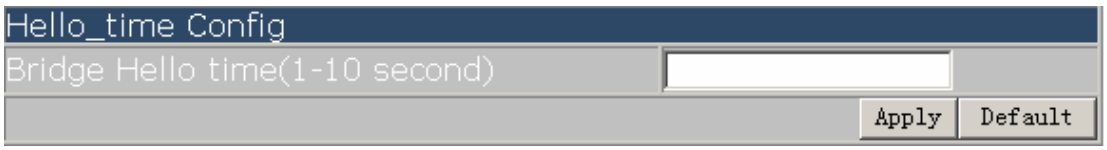


10.5.3.3 Hello_time configuration

Click “MSTP control” to enter MSTP Global control, then "Hello_time Config".

Set the Hello time for the switch.

Set MSTP Hello time to 5 seconds in Global Mode.

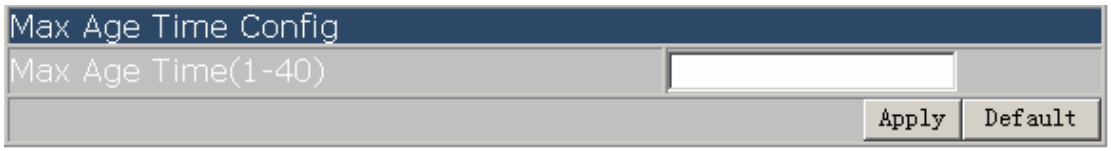


10.5.3.4 Set the max age time for BPDU information in the switch

Click “MSTP control”, MSTP Global Control, then enter the switch BPDU message "Max Age Time Config".

Set the max age time for BPDU information in the switch

Set max age time to 25 seconds in Global Mode.

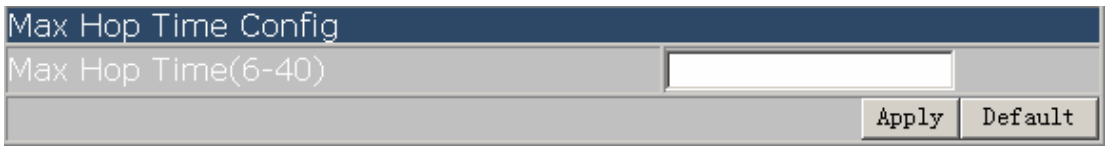


10.5.3.5 Set the max hop count support for BPDU transmitting in MSTP field

Click “MSTP control”, “MSTP Global control”, then set the BPDU "Max Hop Time Config" to support transmission in MSTP field.

Set the max hop count support for BPDU transmitting in MSTP field.

Set the max-hop count to 32.

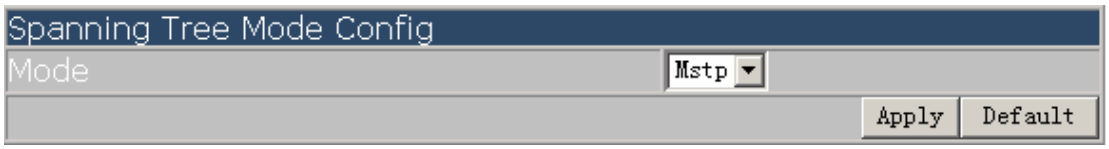


10.5.3.6 Set switch to spanning tree mode

Click “MSTP control”, “MSTP Global control”, enter "Spanning Tree Mode Config" to configure Spanning Tree mode.

Set switch to Spanning Tree mode.

Set the switch to STP mode.

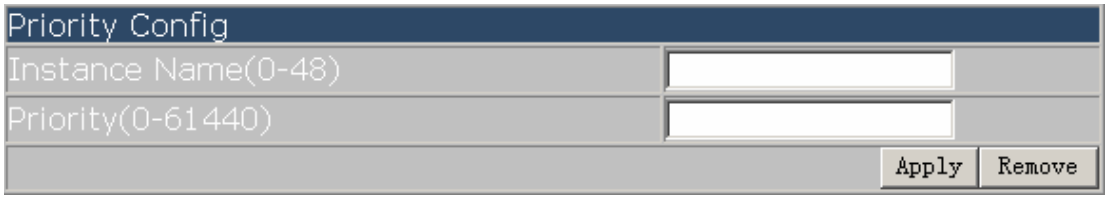


10.5.3.7 Set bridge priority of the specified instance for the switch

Click “MSTP control”, “MSTP Global control”, enter the "Priority Config" to set bridge priority for the switch for the specified instance.

Set bridge priority of the specified instance for the switch

Configure switch instance2 priority to 4096.



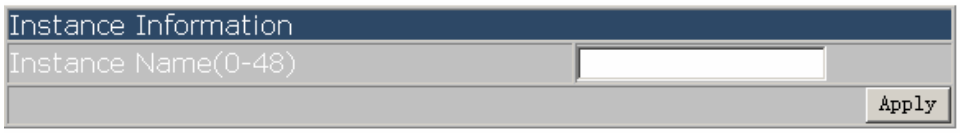
10.5.4 Show MSTP setting

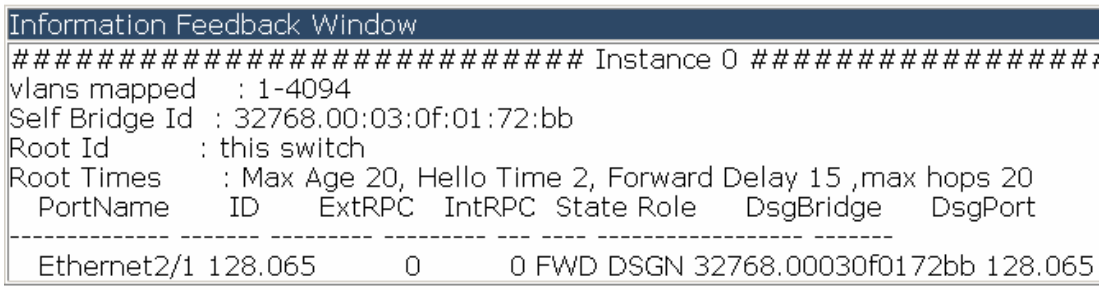
10.5.4.1 Instance information

Click MSTPL control, “show MSTP settings”, enter "Instance Information".

Display MSTP and instances information.

Display Instance0 MSTP information.




Information Feedback Window
############################## Instance 0 ##################
vlans mapped : 1-4094
Self Bridge Id : 32768.00:03:0f:01:72:bb
Root Id : this switch
Root Times : Max Age 20, Hello Time 2, Forward Delay 15 ,max hops 20
PortName ID ExtRPC IntRPC State Role DsgBridge DsgPort
Ethernet2/1 128.065 0 0 FWD DSGN 32768.00030f0172bb 128.065

10.5.4.2 MSTP field information

Click “MSTP control”, “show MSTP setting”, enter "MSTP Field Information".

Display effective MSTP field parameter configurations.

Chapter11 IGMP Snooping Configuration

11.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network devices (such as a routers) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send a IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with a IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and can then decide to forward multicast packets according to the forwarding table.

ES4704BD provides IGMP Snooping and is able to send a query from the switch so that the user can use ES4704BD in IP multicast.

11.2 IGMP Snooping Configuration

11.2.1 IGMP Snooping Configuration Task

1. Enable IGMP Snooping
2. Configure IGMP Snooping
3. Configure sending of IGMP Query

1. Enable IGMP Snooping

Command	Explanation
Global Mode	
ip igmp snooping **no ip igmp snooping**	Enables IGMP Snooping

2. Configure IGMP Snooping

Command	Explanation
Global Mode	

ip igmp snooping vlan <*vlan-id*> **no ip igmp snooping vlan <*vlan-id*>**	Enables IGMP Snooping for specified VLAN
ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> mrouter**	Sets the specified VLAN the port for connecting M-router
ip igmp snooping vlan <*vlan-id*> immediate-leave **no ip igmp snooping vlan <*vlan-id*> immediate-leave**	Enables IGMP Snooping in the specified VLAN to quickly leave multicast group
ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*> interface <*interface –name*> **no ip igmp snooping vlan <*vlan-id*> static <*multicast-ip-addr*>**	Configures a static multicast address and port member to join

3. Configure IGMP to send Query

Command	Explanation
Global Mode	
ip igmp snooping vlan <*vlan-id*> query **no ip igmp snooping vlan <*vlan-id*> query**	Enables IGMP Snooping of a specified VLAN to send a query
ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*> **no ip igmp snooping vlan <*vlan-id*> query robustness**	Sets the robustness parameter for IGMP Snooping Queries of a specified VLAN
ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*> **no ip igmp snooping vlan <*vlan-id*> query interval**	Sets the query interval for IGMP Snooping Query of a specified VLAN
ip igmp snooping vlan <*vlan-id*> query max-response-time <*time-value*> **no ip igmp snooping vlan <*vlan-id*> query max-response-time**	Sets the maximum response time for IGMP Snooping Query of specified VLAN

11.2.2 IGMP Snooping Configuration Command

11.2.2.1 ip igmp snooping

Command: ip igmp snooping
no ip igmp snooping

Function: Enables the IGMP Snooping function in the switch: the "**no ip igmp snooping**"

command disables the IGMP Snooping function.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: Enabling IGMP Snooping allows the switch to monitor multicast traffic in the network and decide which ports will receive multicast traffic.

Example: Enabling IGMP Snooping in Global Mode.

Switch(Config)#ip igmp snooping

11.2.2.2 ip igmp snooping vlan

Command: **ip igmp snooping vlan <*vlan-id*>**
no ip igmp snooping vlan <*vlan-id*>

Function: Enables the IGMP Snooping function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id>**" command disables the IGMP Snooping function for the specified VLAN.

Parameters: **<*vlan-id*>** is the VLAN number.

Command mode: Global Mode

Default: IGMP Snooping is disabled by default.

Usage Guide: IGMP Snooping for the switch must be enabled first to enable IGMP Snooping for the specified VLAN. This command cannot be used with **ip igmp snooping vlan <*vlan-id*> query** command, i.e., either snooping or query can be enabled for one VLAN, but not both.

Example: Enabling IGMP Snooping for VLAN 100 in Global Mode.

Switch(Config)#ip igmp snooping vlan 100

11.2.2.3 ip igmp snooping vlan mrouter

Command: ip igmp snooping vlan <*vlan-id*> mrouter interface <*interface –name*>
no ip igmp snooping vlan <*vlan-id*> mrouter

Function: Specifies a static multicast router port in the VLAN; the "**no ip igmp snooping vlan <*vlan-id*> mrouter**" command deletes the multicast router port.

Parameters: **<*vlan-id*>** is the a specified VLAN number; **<*interface –name*>** is the specified multicast router port number. .

Command mode: Global Mode

Default: No M-Router port is set in the default VLAN.

Usage Guide: M-Router port must be set in a VLAN enabled with IGMP Snooping, or the IGMP packet will be discarded and so IGMP Snooping cannot be performed.

Example: Setting port 1/6 of VLAN 100 to be the M-Router port.

Switch(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/6

11.2.2.4 ip igmp snooping vlan static

Command: ip igmp snooping vlan <*vlan-id*> static <multicast-ip-addr> interface <*interface –name*>

no ip igmp snooping vlan <*vlan-id*> static <multicast-ip-addr>

Function: Enables the IGMP Snooping static multicast group membership: the "**no ip igmp snooping vlan <vlan-id> static <multicast-ip-addr>**" command disables the function.

Parameters: **<*mac-id*>** stands for the specified VLAN number; **<*multicast-ip-addr*>** for multicast MAC address; **<*interface-name*>** for multicast group member port. .

Command mode: Global Mode

Default: No static multicast group is set by default.

Usage Guide: If the static multicast address to be added exists and is a dynamic address, the static address overwrites the dynamic one.

Example: Creating a new static multicast address 224.1.1.1 in VLAN 100 and including port 1/6 in the group.

Switch(Config)#ip igmp snooping vlan 100 static 224.1.1.1 interface ethernet 1/6

Delete static multicast address 224.1.1.1 in VLAN 100.

Switch(Config)#no ip igmp snooping vlan 100 static 224.1.1.1

11.2.2.5 ip igmp snooping vlan immediate-leave

Command: ip igmp snooping vlan <*vlan-id*> immediate-leave

no ip igmp snooping vlan <*vlan-id*> immediate-leave

Function: Enables the IGMP fast leave function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> immediate-leave**" command disables the IGMP fast leave function.

Parameters: **<*vlan-id*>** is the VLAN number specified.

Command mode: Global Mode

Default: This function is disabled by default.

Usage Guide: Enabling IGMP fast leave function speeds up the process for port to leave multicast group. This command is valid only in Snooping, and is not applicable to Query.

Example: Enabling the IGMP fast leave function for VLAN 100.

Switch(Config)#ip igmp snooping vlan 100 immediate-leave

11.2.2.6 ip igmp snooping vlan query

Command: ip igmp snooping vlan <*vlan-id*> query

no ip igmp snooping vlan <*vlan-id*> query

Function: Enables the IGMP Query function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> query**" command disables the Query function.

Parameters: <***vlan-id***> is the VALN number specified.

Command mode: Global Mode

Default: IGMP Query is disabled by default.

Usage Guide: Before enabling the IGMP Query function for the specified VLAN, the switch must have a corresponding VLAN configured and IGMP Snooping enabled. It should be noted that this command cannot be used with **ip igmp snooping vlan <*vlan-id*>** command, i.e., either snooping or query can be enabled for one VLAN, but not both.

Example: Enabling the IGMP Query function for VLAN 100.

Switch(Config)#ip igmp snooping vlan 100 query

11.2.2.7 ip igmp snooping vlan query robustness

Command: ip igmp snooping vlan <*vlan-id*> query robustness <*robustness-variable*>
no ip igmp snooping vlan <*vlan-id*> query robustness

Function: Enables the IGMP Query function for the specified VLAN: the "**no ip igmp snooping vlan <vlan-id> query robustness**" command restores the default setting.

Parameters: <***vlan-id***> is the specified VLAN number; <***robustness-variable***> is robustness parameter, the valid range is 2 to 10.

Command mode: Global Mode

Default: The default robustness parameter is 2.

Usage Guide: A larger robustness parameter means worse network conditions; smaller robustness parameter means better network conditions. The user can set the robustness parameter according to their network conditions.

Example: Setting the robustness parameter for the IGMP Query of VLAN 100 to 3.

Switch(Config)#ip igmp snooping vlan 100 query robustness 3

11.2.2.8 ip igmp snooping vlan query interval

Command: ip igmp snooping vlan <*vlan-id*> query interval <*interval-value*>
no ip igmp snooping vlan <*vlan-id*> query interval

Function: Sets the IGMP Query interval for the specified VLAN; the "**no ip igmp snooping vlan <vlan-id> query interval**" command restores the default setting.

Parameters: <***vlan-id***> is the specified VLAN number; <***interval-value***> is the query interval, valid range is 1 to 65535.

Command mode: Global Mode

Default: The default interval is 125 seconds.

Example: Setting the IGMP Query interval for VLAN 100 to 60 seconds.

Switch(Config)#ip igmp snooping vlan 100 query interval 60

11.2.2.9 ip igmp snooping vlan query max-response-time

Command: ip igmp snooping vlan <*vlan-id*> query max-response-time <*time-value*>
no ip igmp snooping vlan <*vlan-id*> query max-response-time

Function: Sets the maximum IGMP Query response time for the specified VLAN; the "**no ip igmp snooping vlan <vlan-id> query max-response-time**" command restores the default setting.

Parameters: <***vlan-id***> is the specified VLAN number; <***time-value***> is maximum query response time, valid range is 10 to 25.

Command mode: Global Mode

Default: The maximum response time is 10 seconds.

Example: Setting the maximum IGMP Query response time of VLAN 100 to 12 seconds.

Switch(Config)#ip igmp snooping vlan 100 query max-response-time 12

11.3 IGMP Snooping Example

Scenario 1. IGMP Snooping function

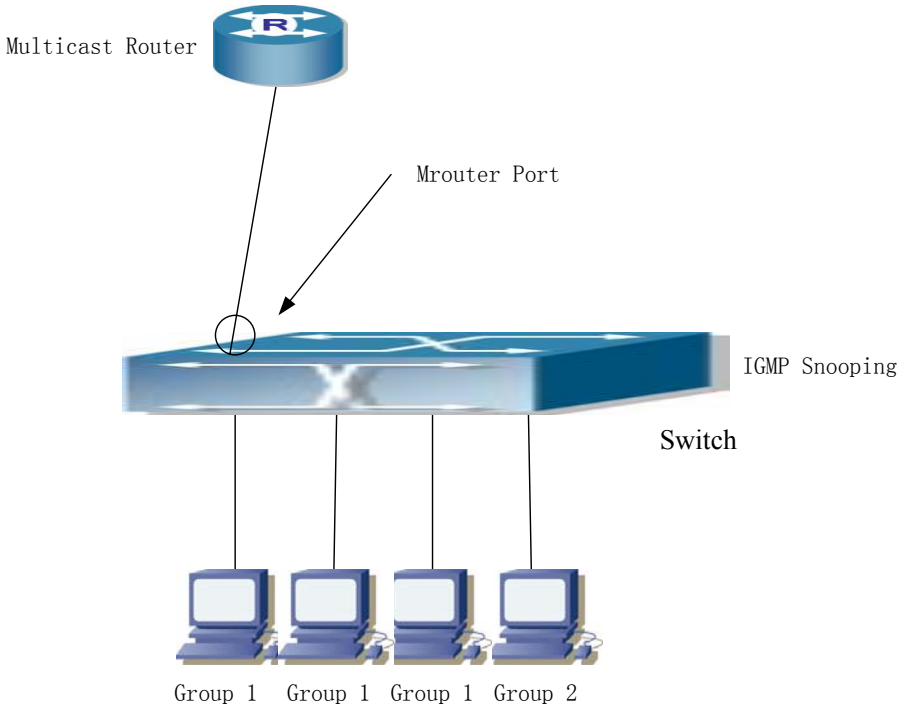


Fig 11-1 Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12 on slot 1. Four hosts are connected to port 2, 6, 10, 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, If IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100 and set port 1 of VLAN 100 to be the M-Router port.

The configuration steps are listed below:

Switch#config

Switch(Config)#ip igmp snooping

Switch(Config)#ip igmp snooping vlan 100

Switch(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1

Multicast Configuration

Suppose two programs are provided in the Multicast Server using multicast address Group1 and Group2, three of four hosts running multicast applications are connected to port 2, 6, 10 plays program1, while the host is connected to port 12 plays program 2.

IGMP Snooping listening result:

The multicast table built by IGMP Snooping in VLAN 100 indicates ports 1, 2, 6, 10 in Group1 and ports 1, 12 in Group2.

All the four hosts can receive the program of their choice: ports 2, 6, 10 will not receive the traffic of program 2 and port 12 will not receive the traffic of program 1.

Scenario 2. IGMP Query

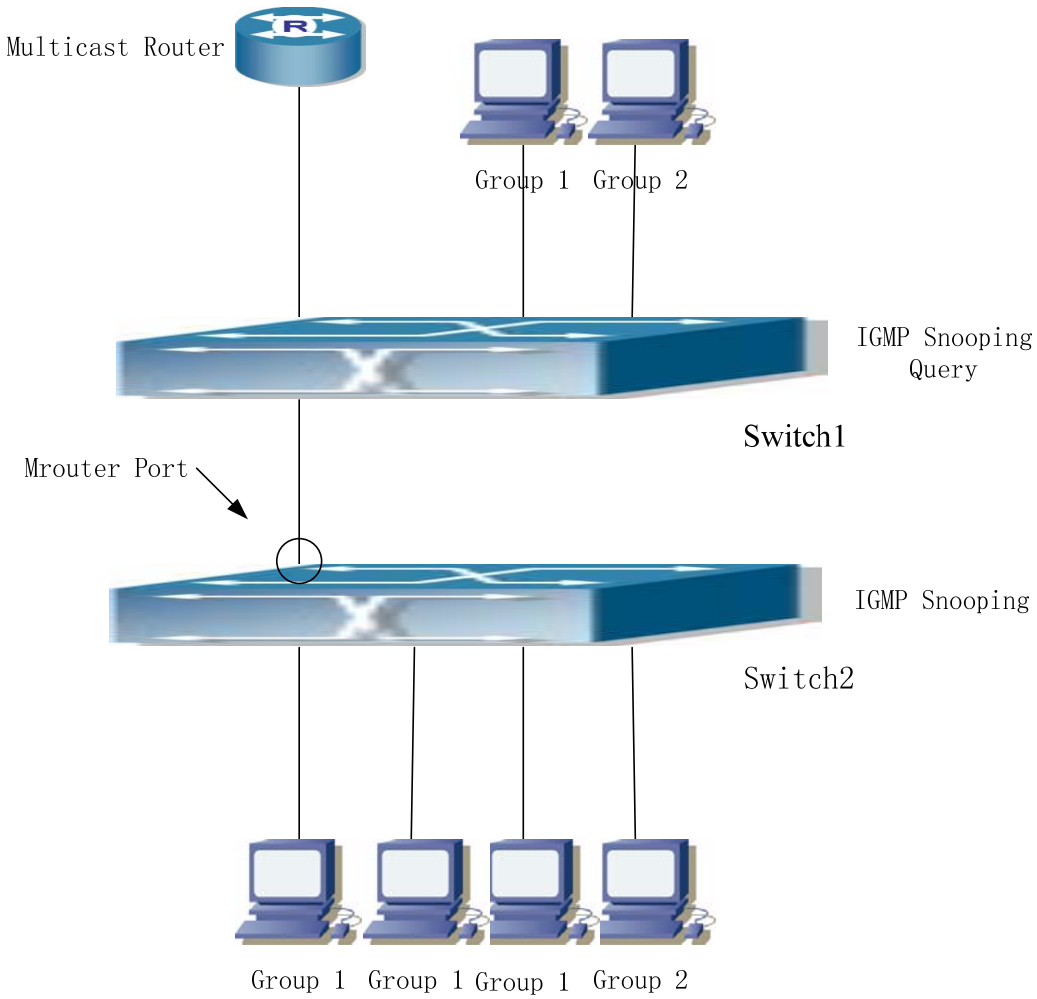


Fig 11-2 The switches as IGMP Queriers

The configuration of Switch2 is the same as the switch in scenario 1, Switch1 takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in Switch1, including ports 1, 2, 6, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. In order to send Query at regular interval, IGMP query must enabled in Global mode and in VLAN60.

The configuration steps are listed below:

Switch1#config
Switch1(Config)#ip igmp snooping
Switch1(Config)#ip igmp snooping vlan 60 query

Switch2#config
Switch2(Config)#ip igmp snooping
Switch2(Config)#ip igmp snooping vlan 100
Switch2(Config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/1

Multicast Configuration

The same as scenario 1.

IGMP Snooping listening result:

Similar to scenario 1.

11.4 IGMP Snooping Troubleshooting Help

11.4.1 Monitor and Debug Commands

11.4.1.1 show ip igmp snooping

Command: show ip igmp snooping [vlan <*vlan-id*>]

Parameters: <*vlan-id*> is id of VLAN to display the IGMP Snooping information.

Command mode: Admin Mode

Usage Guide: If VLAN id is not specified, then summary information for IGMP Snooping and Query in all VLAN will be displayed. If VLAN id is specified, then detailed information for IGMP Snooping and Query of the specified VLAN will be displayed.

Example:

1. Displaying the summary information of IGMP Snooping and Query for the switch.

Switch#show ip igmp snooping
igmp snooping status :Enabled

IGMP information for VLAN 1:

igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)----------

IGMP information for VLAN 2:

igmp snooping vlan status :Enabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

IGMP information for VLAN 3:

igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

IGMP information for VLAN 4:
igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

IGMP information for VLAN 511:

igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

IGMP information for VLAN 5:

igmp snooping vlan status :Disabled
igmp snooping vlan query :Disabled
igmp snooping vlan mrouter port :(null)

Displayed information	Explanation
igmp snooping status	Whether “igmp snooping” function is enabled.
igmp snooping vlan status	“igmp snooping” status of all VLANs in the switch (enabled or not)
igmp snooping vlan query	Query status of all VLANs in the switch (enabled or not).
igmp snooping vlan mrouter port	All M-Router port number (if any) of all VLANs in the switch
igmp snooping vlan mrouter state	All M-Router port (if any) status of all VLANs in the switch, this will not be displayed if no M-Router port is specified.

2. Displaying detailed information of IGMP Snooping and Query for VLAN2.

Switch#show ip igmp snooping vlan 2

IGMP information for VLAN 2:

igmp snooping status :Enabled
igmp snooping vlan status :Enabled
igmp snooping vlan mrouter port :Ethernet1/4
igmp snooping vlan mrouter state :UP
igmp snooping vlan mrouter present :Yes
igmp snooping vlan immediate leave :No
igmp snooping vlan query :Disabled
igmp snooping vlan robustness :2
igmp snooping vlan query interval :125
igmp snooping vlan query max response time :10
igmp snooping vlan query TX :0
igmp snooping vlan query SX :2
igmp snooping multicast information:

MAC address Member port list

01-00-5E-7F-28-B3 Ethernet1/5

01-00-5E-7F-30-BD Ethernet1/4 Ethernet1/5

Sort by port:

Port State Type Group Address Life

```
--------------------------------------------------------------------------
Ethernet1/4     MEMBERS_PRESENT     Snoop_Group_Addr     239.255.48.189          0
--------------------------------------------------------------------------
Ethernet1/5     MEMBERS_PRESENT     Snoop_Group_Addr     239.255.40.179          0
                MEMBERS_PRESENT     Snoop_Group_Addr     239.255.48.189          0
--------------------------------------------------------------------------
```

Displayed information	Explanation
igmp snooping status	Whether “igmp snooping” function is enabled.
igmp snooping vlan status	“igmp snooping” status of the VLAN (enabled or not)
igmp snooping vlan query	“igmp query” status of the VLAN (enabled or not)
igmp snooping vlan mrouter port	M-Router port number (if any) of the VLAN
igmp snooping vlan mrouter state	All M-Router port (if any) status of all VLANs in the switch, this will not be displayed if no M-Router port is specified
igmp snooping vlan mrouter present	Whether query packets present in the M-Router
igmp snooping vlan query TX	Query packet number sent by the VLAN
igmp snooping vlan query SX	Query packet number received by the VLAN
igmp snooping multicast mac	Multicast addresses learnt by the IGMP Snooping forward table.
igmp snooping multicast port	The member port name corresponding to each multicast MAC address in the IGMP Snooping forward table.

11.4.1.2 show mac-address-table multicast

Command: show mac-address-table multicast [vlan <*vlan-id*>]

Function: Displays information for the multicast MAC address table.

Parameters: <*vlan-id*> is the VLAN ID to be included in the display result.

Command mode: Admin Mode

Default: Multicast MAC address-port mapping is not displayed by default.

Usage Guide: This command can be used to display the multicast MAC address table for the current switch.

Example: Displaying the multicast mapping for VLAN100.

```
Switch#show mac-address-table multicast vlan 100
Vlan Mac Address                    Type       Ports
---- --------------------------- ------- ---------------------------------------
100    01-00-5e-01-01-01                MULTI     IGMP        Ethernet1/2
```

11.4.1.3 debug igmp snooping

Command: debug ip igmp snooping

no debug ip igmp snooping

Function: Enables the IGMP Snooping debug function; the “ **no debug ip igmp snooping”**

command disables this debug function**.**

Command mode: Admin Mode

Default: IGMP Snooping debug is disabled by default.

Usage Guide: Use this command to enable IGMP Snooping debug, IGMP packet processing information can be displayed.

Example: Enabling IGMP Snooping debug.

Switch#debug ip igmp snooping

11.4.2 IGMP Snooping Troubleshooting Help

- ☞ IGMP Snooping function cannot be used with IGMP Query, Snooping is not available when Query is enabled. The user must make sure which, IGMP Snooping or IGMP Query, is to be enabled.
- ☞ When IGMP Snooping is used, M-Router port must be specified in the corresponding VLAN, or the switch cannot perform IGMP Snooping properly.

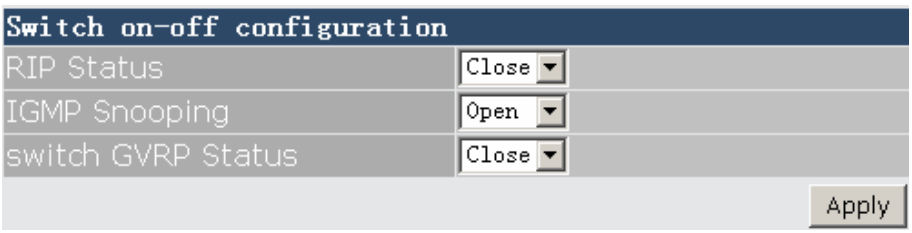
11.5 WEB MANAGEMENT

Click on the IGMP Snooping configuration, the IGMP Snooping configuration node and the IGMP Snooping static multicast configuration node will be expanded. The IGMP Snooping configuration screen is used for the configuration and display of the IGMP snooping & query. While the IGMP Snooping static multicast configuration page is used for configuring the static address and displaying all the IGMP snooping and every setting for VLAN.

11.5.1 Turning on the IGMP snooping function

Before we proceed with the configuration of IGMP Snooping configuration screen, the IGMP snooping function must be enabled on first. The procedure is as follows:

- Click “the switch basic configuration” expand the configuration tree
- Click on “Switch on-off configuration” to turn on the switch configuration page
- Under the IGMP snooping attribute choose open and then click on the Apply button. This is equivalent to the CLI command 11.2.2.1



11.5.2 IGMP snooping configuration

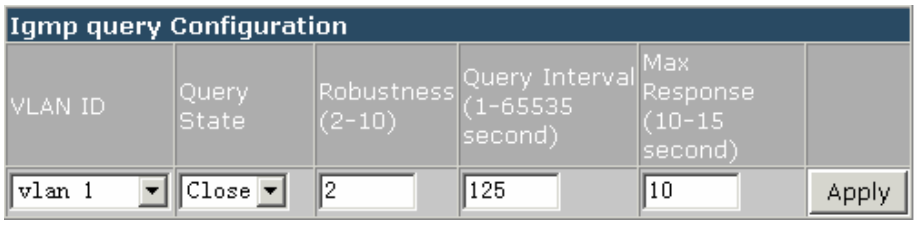
Click “IGMP Snooping configuration” node to enter the IGMP Snooping configuration page. This page is divided into 3 sections: query configuration, snooping configuration and configuration display.

11.5.2.1 Query configuration

The description for each parameter is as follows:

- VLAN ID－configures the vlan ID for query
- Query State－query status: enables or displays. Equivalent to the CLI command 11.2.2.6
- Robustness－This is equivalent to the CLI command 11.2.2.7
- Query Interval－The interval time for query. This is equivalent to the CLI command 11.2.2.8
- Max Response－The maximum value for response time. Equivalent to the CLI command 11.2.2.9

To configure query, select VLAN from the VLAN ID list, under Query State choose Open, configure the other parameters, click Apply.

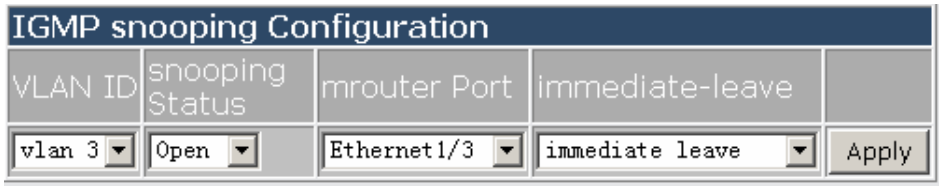


11.5.2.2 Snooping configuration

The description for each parameter is as following:

- VLAN ID－configure the vlanID for snooping
- snooping status－Open or Close. This is equivalent to the CLI command 11.2.2.2
- mrouter Port－This is equivalent to the CLI command 11.2.2.3
- Immediate-leave－Immediate-leave or no Immediate-leave. This is equivalent to the CLI command 11.2.2.5

To configure snooping, select the Vlan from VLAN ID list, set snooping status to open, configure the other parameters and click Apply.



11.5.2.3 Configuration display

When the configuration had been executed as described in the above section, the display is as follows:

IGMP Configuration							
VLAN ID	snooping State	Query State	Robustness	Query Interval	Max Response	mrouter Port	immediate-leave
1	Close	Close	0	0	0	(null)	Close
2	Close	Open	2	125	10	(null)	Close
3	Open	Close	0	0	0	Ethernet1/3	Open

11.5.3 IGMP snooping static multicast configuration

Click “IGMP Snooping static multicast configuration” to enter the configuration screen. The page is divided into configuration section and display section.

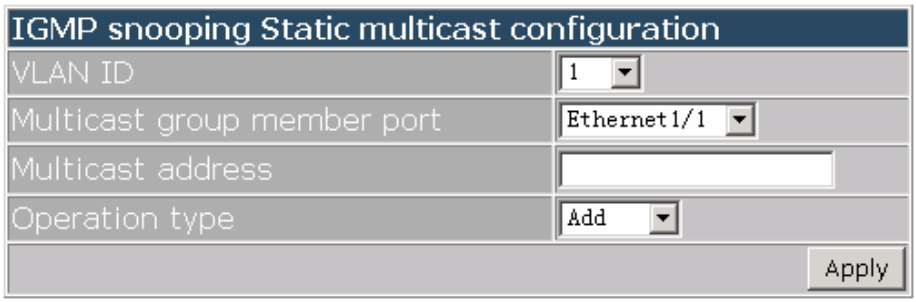
11.5.3.1 IGMP snooping static multicast configuration

The description for each parameter is as follows:

- VLAN ID－configures the Vlan ID
- Multicast group member port
- Multicast address－configures the multicast address.
- Operation type－adds or removes the static multicast member

This is equivalent to the CLI command 11.2.2.4.

To add the static multicast address, select the VLAN to be configured from the VLAN ID list. Select a port from the Multicast group member port, fill in the Multicast address, choose Add from the Operation type, click on Apply.



11.5.3.2 IGMP snooping display

Select a VLAN from the VLAN ID list in the static multicast configuration. The display section will display the IGMP snooping information for that particular VLAN

This is equivalent to the CLI command 11.4.1.1.

Information display

```
IGMP information for VLAN 1:

igmp snooping status                : Enabled
igmp snooping vlan status           : Enabled
igmp snooping vlan mrouter port     : Ethernet1/1
igmp snooping vlan mrouter state    : UP
igmp snooping vlan mrouter present  : No
igmp snooping vlan immediate leave  : Yes
igmp snooping vlan query            : Disabled
igmp snooping vlan robustness       : 2
igmp snooping vlan query interval   : 125
igmp snooping vlan query response time: 10
igmp snooping vlan query TX         : 0
igmp snooping vlan query SX         : 0
igmp snooping multicast information  :
MAC address          Member port list
-------------------------------------------------------------------------------
01- 00- 5E- 01- 01- 02      Ethernet1/1  Ethernet1/3
-------------------------------------------------------------------------------

Sort by port:

Port         State            Type            Group Address   Life
-------------------------------------------------------------------------------
Ethernet1/3     MEMBERS_PRESENT      Static_Group_Addr    225.1.1.2       0
-------------------------------------------------------------------------------
```

Chapter 12 ACL Configuration

12.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access through the switches, effectively safeguarding the security of networks. The user can lay down a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched: “permit” or “deny”. The user can apply such rules to the incoming or outgoing direction of switch ports, so that data streams in the specific direction of specified ports must comply with the ACL rules assigned.

12.1.1 Access list

Access list is a sequential collection of conditions that corresponds to a specific rule. Each rule consists of filter information and the action when the rule is matched. Information included in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port. Access lists can be categorized by the following criteria:

- Filter information based criterion: IP access list (layer 3 or higher information), MAC access list (layer 2 information), and MAC-IP access list (layer 2 or higher). The current implementation supports IP access list only, the other two functions will be provided later.
- Configuration complexity based criterion: standard and extended, the extended mode allows more specific filtering of information.
- Nomenclature based criterion: numbered and named.

Description of an ACL should cover the above three aspects.

12.1.2 Access-group

When a set of access lists are created, they can be applied to traffic of any direction on all ports. Access-group is the description to a the binding of an access list to the specified direction on a specific port. When an access-group is created, all packets from in the specified direction through the port will be compared to the access list rule to decide whether to permit or deny access.

12.1.3 Access list Action and Global Default Action

There are two access list actions and default actions: “permit” or “deny”

The following rules apply:

- An access list can consist of several rules. Filtering of packets compares packet conditions to the rules, from the first rule to the first matched rule; the rest of the rules will not be processed.
- Global default action applies only to IP packets in the incoming direction on the ports. For non-incoming IP packets and all outgoing packets, the default forward action is “permit”.
- Global default action applies only when packet flirter is enabled on a port and no ACL is bound to that port, or no binding ACL matches.
- When an access list is bound to the outgoing direction of a port, the action in the rule can only be “deny”.

12.2 ACL configuration

12.2.1 ACL Configuration Task Sequence

1. Configuring access list
   （1） Configuring a numbered standard IP access list
   （2） Configuring an numbered extended IP access list
   （3） Configuring a standard IP access list based on nomenclature
      a) Create an standard IP access list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
   （4） Configuring an extended IP access list based on nomenclature.
      a) Create an extensive IP access list based on nomenclature
      b) Specify multiple “permit” or “deny” rule entries.
      c) Exit ACL Configuration Mode
2. Configuring the packet filtering function
   (1) Enable global packet filtering function
   (2) Configure default action.
3. Bind access list to a specific direction of the specified port.

1. Configuring access list

(1) Configuring a numbered standard IP access list

Command	Explanation
Global Mode	

access list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} **no access list <*num*>**	Creates a numbered standard IP access list, if the access list already exists, then a rule will add to the current access list; the "**no access list <*num*>**" command deletes a numbered standard IP access list.

(2) Configuring a numbered extensive IP access list

Command	Explanation
Global Mode	
access list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered ICMP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered IGMP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered TCP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]	Creates a numbered UDP extended IP access rule; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
access list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]	Creates a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the numbered extended access list of specified number does not exist, then an access list will be created using this number.
no access list <*num*>	Deletes a numbered extensive IP access list

3) Configuring a standard IP access list basing on nomenclature

a. Create a name-based standard IP access list

Command	Explanation
Global Mode	
ip access standard <*name*> **no ip access standard <*name*>**	Creates a standard IP access list based on nomenclature; the "**no ip access standard <*name*>**" command delete the name-based standard IP access list

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Standard IP ACL Mode	
[no] {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}	Creates a standard name-based IP access rule; the "**no**" form command deletes the name-based standard IP access rule

c. Exit name-based standard IP ACL configuration mode

Command	Explanation
Standard IP ACL Mode	
Exit	Exits name-based standard IP ACL configuration mode

4) Configuring an name-based extended IP access list

a. Create an extended IP access list basing on nomenclatur

Command	Explanation
Global Mode	
ip access extended <*name*> **no ip access extended <*name*>**	Creates an extended IP access list basing on nomenclature; the "**no ip access extended <*name*>**" command deletes the name-based extended IP access list

b. Specify multiple "permit" or "deny" rules

Command	Explanation
Extended IP ACL Mode	
[no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based ICMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based IGMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based TCP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based UDP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]	Creates an extended name-based IP access rule for other IP protocols; the "**no**" form command deletes this name-based extended IP access rule

c. Exit extended IP ACL configuration mode

Command	Explanation
Extended IP ACL Mode	
Exit	Exits extended name-based IP ACL configuration mode

2. Configuring packet filtering function

(1) Enable global packet filtering function

Command	Explanation
Global Mode	
Firewall enable	Enables global packet filtering function
Firewall disable	disables global packet filtering function

(2) Configure default action.

Command	Explanation
Global Mode	
Firewall default permit	Sets default action to "permit"
Firewall default deny	Sets default action to "deny"

3. Bind access-list to a specific direction of the specified port.

Command	Explanation
Physical Interface Mode	

ip access-group <*name*> {in|out } **no ip access-group <*name*> {in|out}**	Applies an access list to the specified direction on the port; the "**no ip access-group <*name*> {in|out}**" command deletes the access list bound to the port.

12.2.2 ACL Configuration Commands

12.2.2.1 access-list(extended)

Command: access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]

no access-list <*num*>

Function: Creates a numbered extended IP access rule for specific IP protocol or all IP protocols; if the numbered extended access list of specified number does not exist, then an access list will be created using this number. The "no" form command deletes a numbered extended IP access list.

Parameters: **<*num*>** is the access table number from 100 to 199; **<*sIpAddr*>** is the source IP address in decimal format; **<*sMask* >** is the mask complement of the source IP in decimal format; **<*dIpAddr*>** is the destination IP address in decimal format; **<*dMask*>** is the mask complement of the destination IP in decimal format, 0 for significant bit and 1 for ignored bit; **<*igmp-type*>** is the IGMP type; **<*icmp-type*>** is the ICMP type; **<*icmp-code*>** is the ICMP protocol number; **<*prec*>** is the IP priority from 0 – 7; **<*tos*>** is the tos value from 0 -15; **<*sPort*>** is the source port number from 0 – 65535; **<*dPort*>** is the destination port number from 0 – 65535.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When the user first specifies a specific **<*num*>**, the ACL of this number will be created, and entries can be added to that ACL.

Example: Creating an extensive IP access list numbered as 110. Denying ICMP packets and allowing UDP packets destined for 192.168.0.1, port 32.

Switch(Config)#access list 110 deny icmp any-source any-destination

Switch(Config)#access list 110 permit udp any-source host-destination 192.168.0.1 d-port 32

12.2.2.2 access list(standard)

Command: access list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}

no access list <*num*>

Function: Creates a numbered standard IP access list, if the access list already exists, then a rule will add to the current access list; the "**no access list <*num*>**" command deletes a numbered standard IP access list.

Parameters: <*num*> is the access list number from 1 to 99; **<*sIpAddr*>** is the source IP address in decimal format; **<*sMask* >** is the mask complement for source IP in decimal format.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When the user first specifies a specific **<*num*>**, the ACL of this number will be created, and entries can be added to that ACL.

Example: Creating a standard IP access list numbered 20, allowing packets from 10.1.1.0/24 and denying packets from 10.1.1.0/16.

Switch(Config)#access list 20 permit 10.1.1.0 0.0.0.255

Switch(Config)#access list 20 deny 10.1.1.0 0.0.255.255

12.2.2.3 firewall

Command: firewall { enable | disable}

Function: Enables or disable firewall.

Parameters: Enables for allow firewall function; disable for prevent firewall action.

Default: The firewall is disabled by default.

Command mode: Global Mode

Usage Guide: Access rules can be configured regardless of firewall status. But the rules can only be applied to the specified direction of specified ports when the firewall is enabled. When the firewall is disabled, all ACL bound to the ports will be deleted.

Example: enabling firewall.

Switch(Config)#firewall enable

12.2.2.4 firewall default

Command: firewall default {permit | deny}

Function: sets firewall default action.

Parameters: "**permit**" allows packets to pass through; "**deny**" blocks packets.

Command mode: Global Mode

Default: The default action is "permit".

Usage Guide: This command affects incoming IP packets on the port only, other packets are allowed to pass through the switch.

Example: setting firewall default action to block packets.

Switch(Config)#firewall default deny

12.2.2.5 ip access extended

Command: ip access extended <*name*>

no ip access extended <*name*>

Function: Creates a name-based extended IP access list; the "**no ip access extended <*name*>**" command delete the name-based extended IP access list

Parameters: **<*name*>** is the name for access list, the character string length is 1 – 8, a pure digit sequence is not allowed.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Creating an extensive IP access list named "tcpFlow".

Switch(Config)#ip access list extended tcpFlow

12.2.2.6 ip access standard

Command: ip access standard <*name*>

no ip access standard <*name*>

Function: Creates a name-based standard IP access list; the "**no ip access standard <*name*>**" command delete the name-based standard IP access list (including all entries).

Parameters: **<*name*>** is the name for access list, the character string length is 1 – 8.

Command mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Creating a standard IP access list named "ipFlow".
Switch(Config)#ip access list standard ipFlow

12.2.2.7 ip access-group

Command: ip access-group [<*num*>|<*acl-name*> { in|out }

no ip access-group <*name*> { in|out }

Function: Applies an access list to the incoming direction on the port; the "**no ip access-group <*name*> {in|out}**" command deletes the access list bound to the port.

Parameter: **<*name*>** is the name for access list; the character string length is 1 – 8.

Command mode: Physical Interface Mode

Default: No ACL is bound by default.

Usage Guide: Only one access rule can be bound to a port, application of an access list on the outgoing direction is not supported yet.

Example: Binding access list "aaa" to the incoming direction of the port.

Switch(Config-Ethernet1/1)#ip access-group aaa in

12.2.2.8 permit | deny(extended)

Command: [no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [ack | fin | psh | rst | syn | urg] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port <*sPort*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port <*dPort*>] [precedence <*prec*>] [tos <*tos*>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | <*int*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>]

Function: Creates or deletes a name-based extended IP access rule for a specified IP protocol or all IP protocols.

Parameters: **<*sIpAddr*>** is the source IP address in decimal format; **<*sMask* >** is the mask complement of the source IP in decimal format; **<*dIpAddr*>** is the destination IP address in decimal format; **<*dMask*>** is the mask complement of the destination IP in decimal format, 0 for significant bit and 1 for ignored bit; **<*igmp-type*>** is the IGMP type from 0 to 255; **<*icmp-type*>** is the ICMP type from 1 to 255; **<*icmp-code*>** is the ICMP protocol number from 0 to 255; **<*prec*>** is the IP priority from 0 – 7; **<*tos*>** is the tos value from 0 -15; **<*sPort*>** is the source port number from 0 – 65535; **<*dPort*>** is the destination port number from 0 – 65535.

Command Mode: named-based extended IP ACL configuration mode

Default: No IP address is configured by default.

Example: Creating an extensive IP access list named "udpFlow", denying IGMP packets and allowing UDP packets destined for 192.168.0.1, port 32.

Switch(Config)#ip access list extended udpFlow

Switch(Config-Ext-Nacl-udpFlow)#deny igmp any-source any-destination

Switch(Config-Ext-Nacl-udpFlow)#permit udp any-source host-destination 192.168.0.1 d-port 32

12.2.2.9 permit | deny(standard)

Command: {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}

no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}

Function: Creates a standard name-based IP access rule; the "no" form command deletes the name-based standard IP access rule

Parameters: **<*sIpAddr*>** is the source IP address in decimal format; **<*sMask*>** is the mask complement for source IP in decimal format.

Command Mode: named-based standard IP ACL configuration mode

Default: No IP address is configured by default.

Example: Allowing packets from 10.1.1.0/24 and denying packets from 10.1.1.0/16.

Switch(Config)# ip access list standard ipFlow

Switch(Config-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255

Switch(Config-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

12.3 ACL Example

Scenario 1:

The user has the following configuration requirement: port 1/10 of the switch connects to 10.0.0.0/24 segment, ftp is not desired for the user.

Configuration description:

1. Create a proper ACL
2. Configuring packet filtering function
3. Bind the ACL to the port

The configuration steps are listed below:

Switch(Config)#access list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch(Config)#firewall enable

Switch(Config)#firewall default permit

Switch(Config)#interface ethernet 1/10

Switch(Config-Ethernet1/10)#ip access-group 110 in
Switch(Config-Ethernet1/10)#exit
Switch(Config)#exit
Configuration result.:
Switch#show firewall
Firewall Status: Enable.
Firewall Default Rule: Permit.
Switch#show access lists
access list 110(used 1 time(s))
access list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/10
interface name:Ethernet1/10
the ingress acl use in firewall is 110.

12.4 ACL Troubleshooting Help

12.4.1 ACL Debug and Monitor Commands

12.4.1.1 show access lists

Command: show access lists [<*num*>|<*acl-name*>]
Function: Displays the access list configured.
Parameters: <***acl-name***> is the specified access list naming string; <***num***> is the specified access list number.
Default: N/A.
Command mode: Admin Mode
Usage Guide: When access list name is not specified, all access list will be displayed; used x time(s) indicates the number the ACL is referred to.
Example:
Switch#show access lists
access list 10(used 0 time(s))
access list 10 deny any-source

access list 100(used 1 time(s))
access list 100 deny ip any-source any-destination
access list 100 deny tcp any-source any-destination

Displayed information	Explanation
access list 10(used 0 time(s))	Numbered ACL10, reference time: 1
access list 10 deny any-source	Denies all IP packets passage
access list 100(used 1 time(s))	Numbered ACL100, reference time: 1.
access list 100 deny ip any-source any-destination	Denies IP packets of any source addresses and destination addresses.
access list 100 deny tcp any-source any-destination	Denies TCP packets of any source IP addresses and destination IP addresses.

12.4.1.2 show access-group

Command: show access-group [interface <*name*>]

Function: Displays ACL binding information for the port.

Parameters: <*name*> is the port name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: If no port is specified, then ACL bound in all ports will be displayed.

Example:

Switch#show access-group

interface name:Ethernet1/2

Ingress access-list used is 111.

interface name:Ethernet1/1

Ingress access-list used is 10.

Displayed information	Explanation
interface name:Ethernet1/2	Binding information of Ethernet port 1/2.
Ingress access list used is 111.	Numbered extended ACL 111 bound to the incoming direction of Ethernet port 1/2.
interface name:Ethernet1/1	Binding information of Ethernet port 1/1.
Ingress access list used is 10.	Numbered standard ACL 10 bound to the incoming direction of Ethernet port 1/1.

12.4.1.3 show firewall

Command: show firewall

Function: Displays packet filtering configuration information.

Parameters: N/A.

Default: N/A.

Command mode: Admin Mode

Usage Guide:

Example:

Switch#show firewall

Firewall Status: Enable.

Firewall Default Rule: Permit.

Displayed information	Explanation
Firewall Status: Enable.	Enables packet filtering function
Firewall Default Rule: Permit.	The default action for packet filtering is "permit"

12.4.2 ACL Troubleshooting Help

- Checking for entries in the ACL is done in a top-down order and ends whenever an entry is matched.
- Default rule will be used only if no ACL is bound to the specific direction of the port, or no ACL entry is matched.
- Applies to IP packets incoming on all ports, and has no effect on other types of packets.
- One port can bound to only one incoming ACL.
- The number of ACLs that can be successfully bound depends on the content of the ACL bound and the hardware resource limit. Users will be prompted if an ACL cannot be bound due to hardware resource limitation.
- If an access list contains same filtering information but conflicting action rules, binding to the port will fail with an error message. For instance, configuring "permit tcp any-source any-destination" and "deny tcp any-source any-destination" at the same time is not permitted.
- Viruses such as "worm.blaster" can be blocked by configuring ACL to block certain ICMP packets.

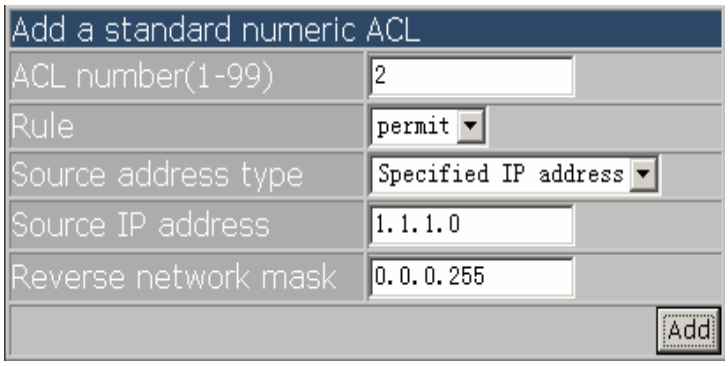
12.5 WEB MANAGEMENT

By clicking the ACL configuration icon, it will open up the ACL sub-sections which include the following parts:

- Numeric ACL Configuration – Standard and Extended types
- ACL Name Configuration – Standard and Extended types
- Filter Configuration -- enable global configuration and the default action to bind ACL to the ports

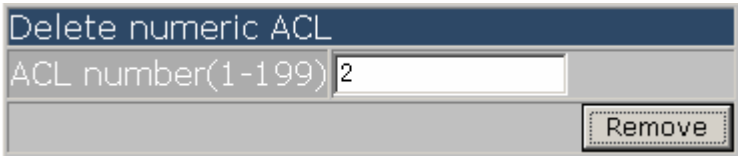
12.5.1 Numeric standard ACL configuration

Click “Numeric ACL Configuration”, and then “Add Standard Numeric ACL” section to enter the configuration page. Equals to its CLI command of 12.2.2.2. The explanations of each section are:
ACL number – 1- 99
Rule – permit or deny
Source address type – Specified IP address or any randomly allocated IP address
Source IP address
Reverse network mask
Specify the number in the ACL number section and the relative values in the other 4 sections, then click “Add”, the users can then add the new Numeric Standard IP ACL.



12.5.2 Delete numeric IP ACL

Click “Numeric ACL Configuration”, and then “Delete Numeric ACL” section to enter the configuration page, it is equals to CLI command of 12.2.2.1 and 12.2.2.2. The explanations of each section are:
ACL number (1-199)
To delete the Numeric ACL, just simply specify the number of ACL and then click the “Remove”.



12.5.3 Configure the numeric extended ACL

There are several extended numeric extended ACLs available:

- Add ICMP numeric extended ACL
- Add IGMP numeric extended ACL
- Add TCP numeric extended ACL
- Add UDP numeric extended ACL
- Add numeric extended ACL for other protocols

By clicking the icons, it will enter the related configuration page which equals to its CLI command of 12.2.2.1

There are several sub-sections in this category：

- ACL number (100-199)
- Rule － permit or deny
- Source address type － Specified IP address or any randomly allocated IP address
- Source IP address
- Reverse network mask
- Target address type － Specified IP address or any randomly allocated IP address
- Destination IP address
- Reverse network mask
- IP precedence
- TOS

Regarding “ICMP numeric extended ACL”, there are two sub-categories:

- ICMP type
- ICMP code

Regarding “IGMP numeric extended ACL”, there is one sub-category:

- IGMP type

Regarding “TCP numeric extended ACL”, there are three sub-categories:

- Source port
- Target port
- TCP sign

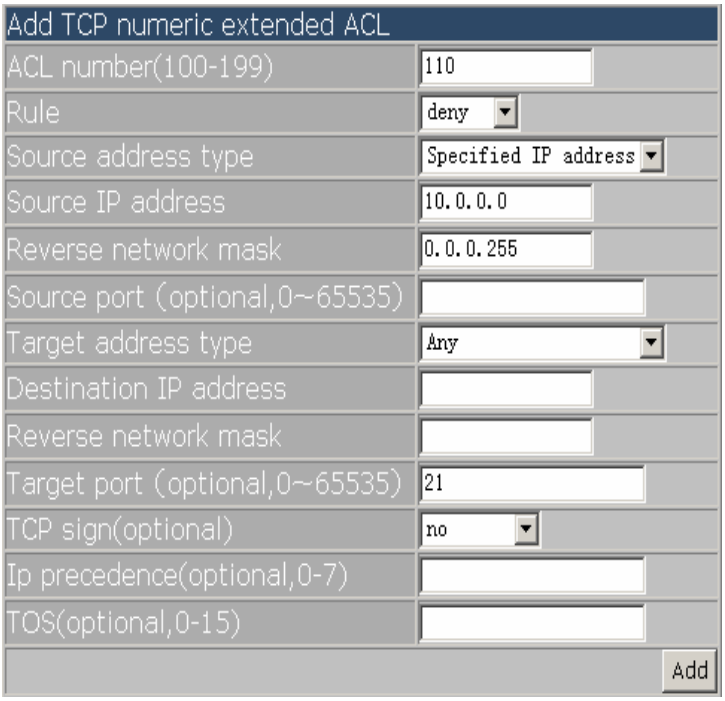
Regarding “UDP numeric extended ACL”, there are two sub-categories:

- Source port
- Target port

Regarding “numeric extended ACL for other protocols”, there is one sub-category: Matched protocol.

- Matched protocol － includes IP, EIGRP, OSPF, IPINIP and Input Protocol manually. If user selects to input manually, they can just simply key-in the protocol number in the right hand side of icon.

Example: a user wants to configure the “ Add TCP numeric extended ACL” with the ACL number of 110, deny the source IP address of 10.0.0.0/24 section, and make the target port is 21. Please refer the following configurations and then click the icon of “Add”.



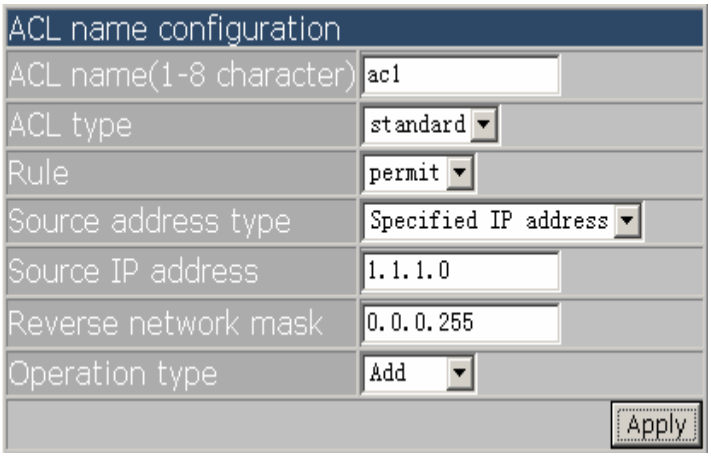
12.5.4 Configure standard ACL name configuration and delete the standard ACL name configuration

Click “ACL name configuration” to open up the sub-sections, next click “ACL name configuration” to enter the configuration page. The way to configure the “ACL name configuration” is the same with “Numeric ACL Configuration”. The only difference users should change the ACL number to the ACL name. This should be entered in ACL name not ACL number. CLI command: 12.2.2.6

There are seven sub-sections of this:

- ACL name
- ACL type － standard and extended
- Rule － permit and deny
- Source address type － Specified IP address or any randomly allocated IP address Source IP address
- Reverse network mask
- Operation type －Add or Remove

To add a numeric ACL, specify the ACL name and related value, select the “add” in the Operation type and then click “Apply”.



12.5.5 Configure extended ACL name configuration

Click "ACL name configuration", the configuration sections will then be shown. There are 6 types of extended ACL name configurations:

- IP extended ACL name configuration
- ICMP extended ACL name configuration
- IGMP extended ACL name configuration
- TCP extended ACL name configuration
- UDP extended ACL name configuration
- Other protocols extended ACL name configuration

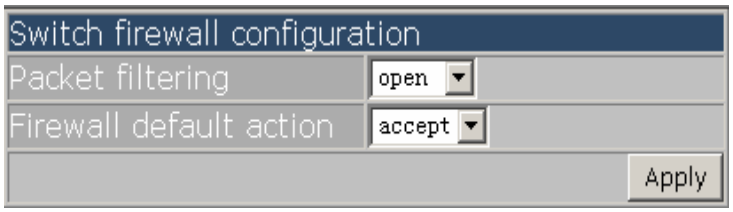
Click the related the configuration web page, the configuration is the same with it is with numeric extended ACL. The only difference is the ACL number needs to be changed to ACL name, and entered into the ACL name rather than number. CLI command: 12.2.2.5.

12.5.6 Firewall configuration

Click "Filter Configuration", and then "Firewall Configuration" to enter the configuration page. The detailed explanation is as follows:

- Packet filtering – "open" to enable or "close" to disable. Equals CLI command: 12.2.2.3
- Firewall default action – "accept" means to allow the packet to pass through and "refuse" to deny the packet. CLI command: 12.2.2.4

To enable or disable, users need to click "Apply" to confirm the command.



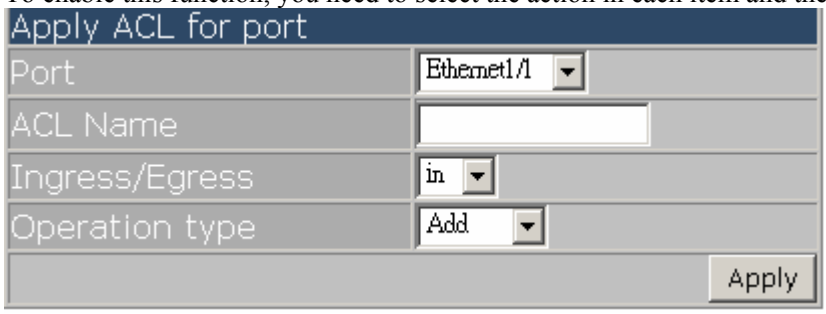
12.5.7 ACL port binding

Click “Filter configuration”, and then select “ACL port binding” to enter the configuration page. Equal to CLI command: 12.2.2.7

There are five items in this section.

- Port – the target port to bind to ACL
- ACL name – the target ACL name to bind
- Ingress/Egress – the target direction to bind
- Operation type – “Add” or “Remove”

To enable this function, you need to select the action in each item and then click “Apply”.



Chapter 13 Port Channel Configuration

13.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first. Port Group is a group of physical ports in the configuration level, only physical ports in the Port Group can take part in link aggregation and become a member port of a Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) of the same properties to a logical port. Port Channel is a collection of physical ports and used logically as one physical port. Port Channel can be used as a normal port by the user, and can not only add network's bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

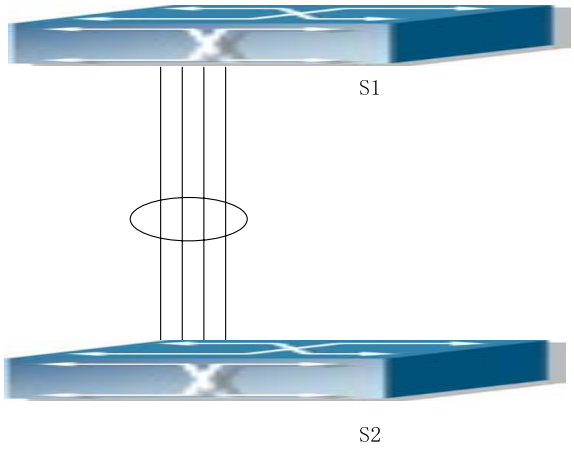


Fig 13-1 Port aggregation

As shown in the above figure13-1，S1 is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from S1 needs to be transferred to S2 through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address.The calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through a traffic allocation algorithm. This algorithm is carried out by the hardware.

ES4704BD offers 2 methods for configuring port aggregation: manual Port Channel creation and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation. Port aggregation can only be performed on ports in full-duplex mode.

For Port Channel to work properly, member ports of the Port Channel must have the same properties as follows:

- ☞ All ports are in full-duplex mode.
- ☞ Ports are of the same speed.
- ☞ All ports are Access ports and belong to the same VLAN or are all Trunk ports.
- ☞ If the ports are Trunk ports, then their "Allowed VLAN" and "Native VLAN" property should also be the same.

If Port Channel is configured manually or dynamically on ES4704BD, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If spanning tree is enabled in the switch, spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. ES4704BD series allow physical port aggregation of any two switches, maximum 8 port groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. ES4704BD has a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical port configuration mode.

13.2 Port Channel Configuration

13.2.1 Port Channel Configuration Task Sequence

1. Create a port group in Global Mode.
2. Add ports to the specified group from the Port Mode of respective ports.
3. Enter port-channel configuration mode.

1. Creating a port group

Command	Explanation
Global Mode	
port-group <*port-group-number*> [load-balance { src-mac | dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}] **no port-group <*port-group-number* > [load-balance]**	Creates or deletes a port group and sets the load balance method for that group.

2. Add physical ports to the port group

Command	Explanation
Interface Mode	
port-group <*port-group-number*> mode {active|passive|on} **no port-group <*port-group-number*>**	Adds ports to the port group and sets their mode.

3. Enter port-channel configuration mode.

Command	Explanation
Global Mode	
interface port-channel <*port-channel-number*>	Enters port-channel configuration mode.

13.2.2 Port Channel Configuration Commands

13.2.2.1 port-group

Command: port-group <*port-group-number*> [load-balance { src-mac|dst-mac | dst-src-mac | src-ip| dst-ip|dst-src-ip}]

no port-group <*port-group-number*> [load-balance]

Function: Creates a port group and sets the load balance method for that group. If no method is specified, the default load balance method is used. The "**no port-group <*port-group-number*> [load-balance]**" command deletes that group or restores the default load balance setting. Enter "load-balance" for restoring default load balance, otherwise, the group will be deleted.

Parameters: <*port-group-number*> is the group number of a port channel from 1 to 8, if the group number is already exist, an error message will be given. **dst-mac** performs load balancing according to destination MAC; **src-mac** performs load balance according to source MAC; **dst-src-mac** performs load balancing according to source and destination MAC; **dst-ip** performs load balancing according to destination IP; **src-ip** performs load balancing according to source IP; **dst-src-ip** performs load balancing according to destination and source IP. If a port group has formed a port-channel, the load balance setting cannot be modified, please set the load balance mode before port-channel.

Default: Switch ports do not belong to a port channel by default; LACP not enabled by default.

Command mode: Global Mode

Example: Creating a port group and setting the default load balance method.

Switch(Config)# port-group 1

Delete a port group.

Switch(Config)#no port-group 1

13.2.2.2 port-group mode

Command: port-group <*port-group-number*> mode {active|passive|on}

no port-group <*port-group-number*>

Function: Adds a physical port to port channel, the "**no port-group <*port-group-number*>**" removes specified port from the port channel.

Parameters: **<*port-group-number*>** is the group number of port channel, from 1 to 8; **active** enables LACP on the port and sets it in Active mode; **passive** enables LACP on the port and sets it in Passive mode; **on** forces the port to join a port channel without enabling LACP.

Command mode: Interface Mode

Default: Switch ports do not belong to a port channel by default; LACP not enabled by default.

Usage Guide: If the specified port group does not exist, a group will be created first to add the ports. All ports in a port group must be added in the same mode, i.e., all ports use the mode used by the first port added. Adding a port in "on" mode is a "forced" action, which means the local end switch port aggregation does not rely on the information of the other end, port aggregation will succeed as long as there are 2 or more ports in the group and all ports have consistent VLAN information. Adding a port in "active" or "passive" mode enables LACP. Ports of at least one end must be added in "active" mode, if ports of both ends are added in "passive" mode, the ports will never aggregate.

Example: Under the Port Mode of Ethernet1/1, add current port to "port-group 1" in "active" mode.

Switch(Config-Ethernet1/1)#port-group 1 mode active

13.2.2.3 interface port-channel

Command: interface port-channel <*port-channel-number*>

Function: Enters the port channel configuration mode

Command mode: Global Mode

Default:

Usage Guide: On entering aggregated port mode, configuration to GVRP or spanning tree modules will apply to aggregated ports; if the aggregated port does not exist (i.e., ports have not been aggregated), an error message will be displayed and configuration will be saved and will be restored until the ports are aggregated. Note such restoration will be performed only once, if an aggregated group is ungrouped and aggregated again, the initial user configuration will not be restored. If it is configuration for modules, such as shutdown or speed configuration, then the configuration to current port will apply to all member ports in the corresponding port group.

Example: Entering configuration mode for port-channel 1.

Switch(Config)#interface port-channel 1

Switch(Config-If-Port-Channel1)#

13.3 Port Channel Example

Scenario 1: Configuring Port Channel in LACP.

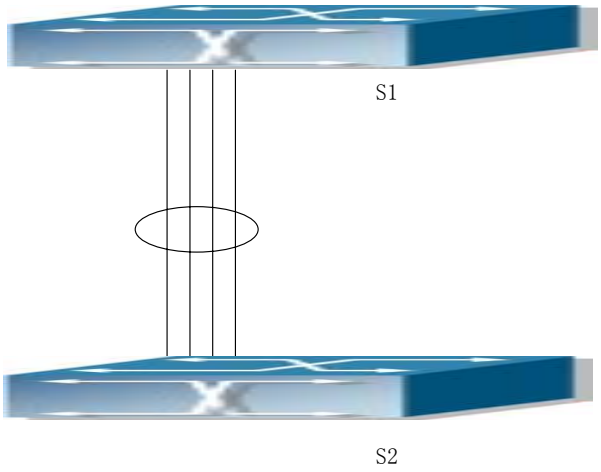


Fig 13-2 Configuring Port Channel in LACP

Example: The switches in the description below are all ES4704BD switches and as shown in the figure, ports 1, 2, 3 of Switch 1 are access ports that belong to vlan1. Add those three port to group1 in active mode; ports 6, 8, 9 of Switch2 are trunk port that allow all add these three ports to group2 in passive mode. All the ports should be connected with cables (four connecting lines in the figure)

The configuration steps are listed below:

Switch1#config
Switch1 (Config)#interface eth 1/1-3
Switch1 (Config-Port-Range)#port-group 1 mode active
Switch1 (Config-Port-Range)#exit
Switch1 (Config)#interface port-channel 1
Switch1 (Config-If-Port-Channel1)#

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 1/6
Switch2 (Config-Ethernet1/6)#port-group 2 mode passive
Switch2 (Config-Ethernet1/6)#exit
Switch2 (Config)# interface eth 1/8-9
Switch2 (Config-Port-Range)#port-group 2 mode passive
Switch2 (Config-Port-Range)#exit
Switch2 (Config)#interface port-channel 2
Switch2 (Config-If-Port-Channel2)#

Configuration result:

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3 of Switch 1 form an aggregated port named “Port-Channel1”, ports 6, 8, 9 of Switch 2 forms an aggregated port named “Port-Channel2”; configurations can be made in their respective aggregated port configuration mode.

Scenario 2: Configuring Port Channel in ON mode.

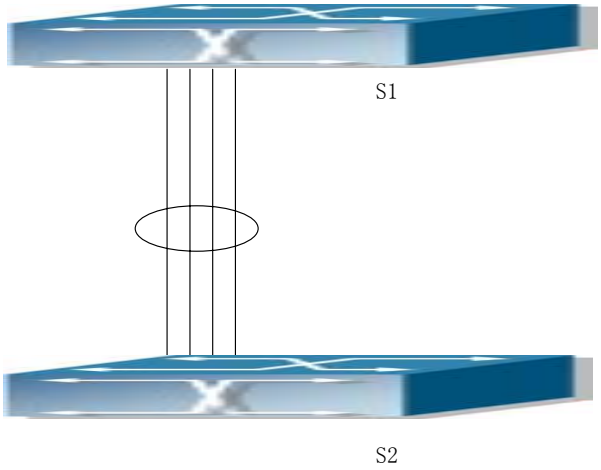


Fig 13-3 Configuring Port Channel in ON mode

Example: As shown in the figure, ports 1, 2, 3 of Switch 1 are access ports that belong to vlan1. Add those three port to group1 in “on” mode.Ports 6, 8, 9 of Switch 2 are trunk port that allow all, add the these three ports to group2 in “on” mode.

The configuration steps are listed below:

Switch1#config
Switch1 (Config)#interface eth 1/1
Switch1 (Config-Ethernet1/1)# port-group 1 mode on
Switch1 (Config-Ethernet1/1)#exit
Switch1 (Config)#interface eth 1/2
Switch1 (Config-Ethernet1/2)# port-group 1 mode on
Switch1 (Config-Ethernet1/2)#exit
Switch1 (Config)#interface eth 1/3
Switch1 (Config-Ethernet1/3)# port-group 1 mode on
Switch1 (Config-Ethernet1/3)#exit

Switch2#config
Switch2 (Config)#port-group 2
Switch2 (Config)#interface eth 1/6

Switch2 (Config-Ethernet1/6)#port-group 2 mode on
Switch2 (Config-Ethernet1/6)#exit
Switch2 (Config)# interface eth 1/8-9
Switch2 (Config-Port-Range)#port-group 2 mode on
Switch2 (Config-Port-Range)#exit

Configuration result:

Add ports 1, 2, 3 of Switch 1 to port-group 1 in order, and we can see joining a group in "on" mode is completely forced action, switch in other ends won't exchange LACP PDU to complete aggregation. Aggregation finishes immediately when the command to add port 2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 3 joins port-group 1, port-channel 1 of port 1 and 2 are ungrouped and re-aggregate with port 3 to form port-channel 1. (it should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregated to form a new group. Now all three ports in both Switch 1 and Switch 2 are aggregated in "on" mode and become an aggregated port respectively.

13.4 Port Channel Troubleshooting Help

13.4.1 Monitor and Debug Commands

13.4.1.1 show port-group

Command: show port-group [<*port-group-number*>] {brief | detail | load-balance | port | port-channel}

Parameters: <*port-group-number*> is the group number of port channel to be displayed, from 1 to 8; **"brief"** displays summary information; **"detail"** displays detailed information; **"load-balance"** displays load balance information; **"port"** displays member port information; **"port-channel"** displays port aggregation information.

Command mode: Admin Mode

Usage Guide: If "port-group-number" is not specified, then information for all port groups will be displayed.

Example: Adding port 1/1 and 1/2 to port-group 1.

1. Display summary information for port-group 1.

Switch#show port-group 1 brief
Port-group number : 1
Number of ports in porg-group : 2 Maxports in port-channel = 8
Number of port-channels : 0 Max port-channels : 1

Displayed information	Explanation

Number of ports in group	Port number in the port group
Maxports	Maximum number of ports allowed in a group
Number of port-channels	Whether aggregated to port channel or not
Max port-channels	Maximum port channel number can be formed by port group.

2. Display detailed information for port-group 1.

Switch# show port-group 1 detail

Sorted by the ports in the group 1:

Ethernet port 1/1 :

both of the port and the agg attributes are not equal

the general information of the port are as follows:

portnumber: 1 actor_port_agg_id:0 partner_oper_sys:0x000000000000

partner_oper_key: 0x0001 actor_oper_port_key: 0x0101

mode of the port: ACTIVE lacp_aware: enable

begin: FALSE port_enabled: FALSE lacp_ena: FALSE ready_n: TRUE

the attributes of the port are as follows:

mac_type: ETH_TYPE speed_type: ETH_SPEED_100M

duplex_type: FULL port_type: ACCESS

the machine state and port state of the port are as the follow

mux_state: DETCH rcvm_state: P_DIS prm_state: NO_PER

actor_oper_port_state : L_A___F_

partner_oper_port_state: _TA___F_

Ethernet port 1/2 :

both of the port and the agg attributes are not equal

the general information of the port are as follows:

portnumber: 2 actor_port_agg_id:0 partner_oper_sys:0x000000000000

partner_oper_key: 0x0002 actor_oper_port_key: 0x0102

mode of the port: ACTIVE lacp_aware: enable

begin: FALSE port_enabled: FALSE lacp_ena: TRUE ready_n: TRUE

the attributes of the port are as follows:

mac_type: ETH_TYPE speed_type: ETH_SPEED_100M

duplex_type: FULL port_type: ACCESS

the machine state and port state of the port are as follows:

mux_state: DETCH rcvm_state: P_DIS prm_state: NO_PER

actor_oper_port_state : L_A___F_

partner_oper_port_state: _TA___F_

Displayed information	Explanation
portnumber	Port number
actor_port_agg_id	The channel number to add the port to. If the port cannot be added to the channel due to inconsistent parameters between the port and the channel, 3 will be displayed.
partner_oper_sys	System ID of the other end.
partner_oper_key	Operational key of the other end.
actor_oper_port_key	Local end operational key
mode of the port	The mode in which port is added to the group
mac_type	Port type: standard Ethernet port and fiber-optical distributed data interface
speed_type	Port speed type: 10Mbps, 100Mbps, 1,000Mbps and 10Gbps.
duplex_type	Port duplex mode: full-duplex and half-duplex
port_type	Port VLAN property: access port or trunk port
mux_state	Status of port binding status machine
rcvm_state	Status of port receiving status machine
prm_state	Status of port sending status machine

3. Display load balance information for port-group 1.

Switch# show port-group 1 load-balance

The loadbalance of the group 1 based on src MAC address.

4. Display member port information for port-group 1.

Switch# show port-group 1 port

Sorted by the ports in the group 1 :

---

the portnum is 1

Ethernet port 1/1 related information:

Actor part

	Administrative	Operational
port number	1	
port priority	0x8000	
aggregator id	0	
port key	0x0100	0x0101
port state		

LACP activety . 1
LACP timeout . .
Aggregation 1 1
Synchronization . .
Collecting . .
Distributing . .
Defaulted 1 1
Expired . .

Partner part

	Administrative	Operational
system	000000-000000	000000-000000
system priority	0x8000	0x8000
key	0x0001	0x0001
port number	1	1
port priority	0x8000	0x8000
port state		
LACP activety	.	.
LACP timeout	1	1
Aggregation	1	1
Synchronization	.	.
Collecting	.	.
Distributing	.	.
Defaulted	1	1
Expired	.	.

Selected Unselected

Displayed information	Explanation
portnumber	Port number
port priority	Port Priority
system	System ID
system priority	System Priority
LACP activety	Whether port is added to the group in “active” mode, 1 for yes.
LACP timeout	Port timeout mode, 1 for short timeout.
Aggregation	Whether aggregation is possible for the port, 0 for independent port that does not allow aggregation.
Synchronization	Whether port is synchronized with the partner end.
Collecting	Whether status of port bound status machine is “collecting” or not.

Distributing	Whether status of port bound status machine is “distributing” or not.
Defaulted	Whether the local port is using default partner end parameter.
Expired	Whether status of port receiving status machine is “expire” or not.
Selected	Whether the port is selected or not..

5. Display port-channel information for port-group1.

Switch# show port-group 1 port-channel

Port channels in the group 1:

Port-Channel: port-channel1

Number of port : 2 Standby port : NULL

Port in the port-channel :

Index Port Mode

---

1 Ethernet1/1 active

2 Ethernet1/2 active

Displayed information	Explanation
Port channels in the group	If port-channel does not exist, the above information will not be displayed.
Number of port	Port number in the port-channel.
Standby port	Port that is in “standby” status, which means the port is qualified to join the channel but cannot join the channel due to the maximum port limit, thus the port status is “standby” instead of “selected”.

13.4.1.2 debug lacp

Command: debug lacp

no debug lacp

Function: Enables the LACP debug function: “**no debug lacp”** command disables this debug function**.**

Command mode: Admin Mode

Default: LACP debug information is disabled by default.

Usage Guide: Use this command to enable LACP debugging so that LACP packet processing information can be displayed.

Example: Enabling LACP debug.

Switch#debug lacp

13.4.2 Port Channel Troubleshooting Help

If problems occur when configuring port aggregation, please first check the following for causes.

- ☞ Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.
- ☞ Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.
- ☞ When port-channel is forced, as the aggregation is triggered manually, the port group will stay unaggregated if aggregation fails due to inconsistent VLAN information. Ports must be added to or removed from the group to trigger another aggregation, if VLAN information inconsistency persists, the aggregation will fail again. The aggregation will only succeed when VLAN information is consistent and aggregation is triggered due to port addition or removal.
- ☞ Verify that port group is configured in the partner end, and in the same configuration. If the local end is set in manual aggregation or LACP, the same should be done in the partner end; otherwise part aggregation will not work properly. Another thing to note is that if both ends are configured with LACP, then at least one of them should be in ACTIVE mode, otherwise LACP packet won't be initialed.
- ☞ LACP cannot be used on ports with Security and IEEE 802.1x enabled.

13.5 WEB MANAGEMENT

Click "Port channel configuration" to open LACP port group configuration and LACP port configuration. LACP port group page will be used to configure and display group while LACP port configuration page will be used to configure and display port group members.

13.5.1 LACP port group configuration

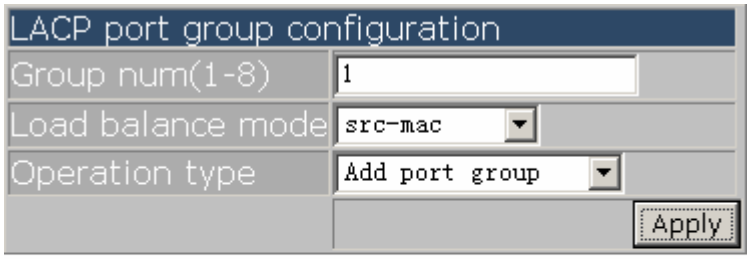
Click "LACP port group configuration" to enter configuration page. Equivalent to CLI command 13.2.2.1.

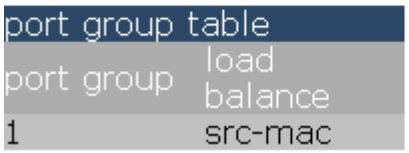
- Group Num: group number
- Load balance mode: includes src-mac, dst-mac, dst-src-mac, src-ip, dst-ip, dst-src-ip
- Operation type: Add port group or Remove port group

Fill in group Num, select load balance mode and select operation type as Add port group. Click

Apply to add the group.

After finishing the group configuration, the configured port information will be shown under the configuration table.





13.5.2 LACP port configuration

Click LACP port configuration to enter configuration page

Equivalent to CLI command 13.2.2.2

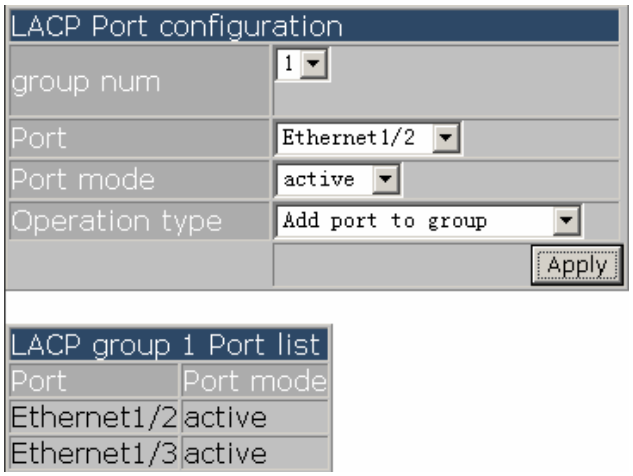
- group num
- Port: will be added or deleted
- Port mode: active, passive or on
- Operation type: add port to group or remove port from group

Fill up group num, select Port and Port mode, operation type as add or to group. Click Apply button to add port into the group.

Display port member

Select a group num in port configuration and the information of port member will be shown under the configuration table. Equivalent to CLI command 13.4.1.1.

- Port: name of port member
- Port mode: active or passive



Chapter 14 DHCP Configuration

14.1 Introduction to DHCP

DHCP [RFC2131] is the acronym for Dynamic Host Configuration Protocol. It is a protocol that assigns dynamically IP addresses to request host from the address pool as well as other network configuration parameters such as default gateway, DNS server, default route and host image file position within the network. DHCP is the enhanced version of BootP. It is a mainstream technology that can not only provide boot information for diskless workstations, but can also release the administrators from manual recording IP allocation and reduce user effort and configuration. Another benefit of DHCP is it can partially ease the pressure on IP demands, when the user of an IP leaves the network, their IP can be assigned to another user.

DHCP is a client-server protocol, the DHCP client requests the network address and configuration parameters from the DHCP server; the server provides the network address and configuration parameters for the clients; if a DHCP server and clients are located in different subnets, DHCP relay is required for DHCP packets to be transferred between the them. The implementation of DHCP is shown below:

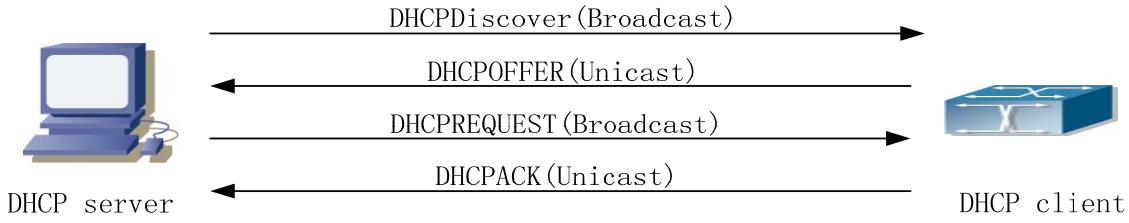


Fig 14-1 DHCP protocol interaction

Explanation:

1. DHCP client broadcasts DHCPDISCOVER packets in the local subnet.
2. On receiving the DHCPDISCOVER packet, DHCP server sends a DHCPOFFER packet along with IP address and other network parameters to the DHCP client.
3. DHCP client broadcast DHCPREQUEST packet with the information for the DHCP server it selected after selecting from the DHCPOFFER packets.
4. The DHCP server selected by the client sends a DHCPACK packet and the client gets an IP address and other network configuration parameters.

The above four steps finish a Dynamic host configuration assignment process. However, if the DHCP server and the DHCP client are not in the same network, the server will not receive the DHCP broadcast packets sent by the client, therefore no DHCP packets will be sent to the client by the server. In this case, a DHCP relay is required to forward such DHCP packets so that the DHCP packets exchange can be completed between the DHCP client and server.

ES4704BD can act as both a DHCP server and a DHCP relay. DHCP server supports not only dynamic IP address assignment, but also manual IP address binding (i.e., specify a specific IP address to a specified MAC address or specified device ID over a long period. The differences and relations between dynamic IP address allocation and manual IP address binding are: 1) IP address

obtained dynamically can be different every time; manually bound IP address will be the same all the time. 2) The lease period of IP address obtained dynamically is the same as the lease period of the address pool and is limited; the lease of manually bound IP address is theoretically endless. 3) Dynamically allocated addresses cannot be bound manually. 4) Dynamic DHCP address pool can inherit the network configuration parameters of the dynamic DHCP address pool of the related segment.)

14.2 DHCP Server Configuration

14.2.1 DHCP Sever Configuration Task Sequence

1. Enable/Disable DHCP server
2. Configure DHCP Address pool
   (1) Create/Delete DHCP Address pool
   (2) Configure DHCP address pool parameters
   (3) Configure manual DHCP address pool parameters
3. Enable logging for address conflicts

1. Enable/Disable DHCP server

Command	Explanation
Global Mode	
service dhcp **no service dhcp**	Enables DHCP server

2. Configure DHCP Address pool

(1) Create/Delete DHCP Address pool

Command	Explanation
Global Mode	
ip dhcp pool <*name*> **no ip dhcp pool <*name*>**	Configures DHCP Address pool

(2) Configure DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
network-address <*network-number*> [mask | prefix-length] **no network-address**	Configures the address scope that can be allocated to the address pool
default-router [address1[address2[…address8]]] **no default-router**	Configures default gateway for DHCP clients

dns-server [address1[address2[…address8]]] **no dns-server**	Configures DNS server for DHCP clients
domain-name <*domain*> **no domain-name**	Configures Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.
netbios-name-server [address1[address2[…address8]]] **no netbios-name-server**	Configures the address for WINS server
netbios-node-type { b-node|h-node|m-node|p-node|<*type-number*>} **no netbios-node-type**	Configures node type for DHCP clients
bootfile <*filename*> **no bootfile**	Configures the file to be imported for DHCP clients on bootup
next-server [address1[address2[…address8]]] **no next-server [address1[address2[…address8]]]**	Configures the address of the server hosting file for importing
option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>} **no option <*code*>**	Configures the network parameter specified by the option code
lease { days [hours][minutes] | infinite } **no lease**	Configures the lease period allocated to addresses in the address pool
Global Mode	
ip dhcp excluded-address <*low-address*> [<*high-address*>] **no ip dhcp excluded-address <*low-address*> [<*high-address*>]**	Excludes the addresses in the address pool that are not for dynamic allocation.

(3) Configure manual DHCP address pool parameters

Command	Explanation
DHCP Address Pool Mode	
hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}] **no hardware-address**	Specifies the hardware address when assigning address manually
host <*address*> [<*mask*> | <*prefix-length*>] **no host**	Specifies the IP address to be assigned to the specified client when binding an address manually

client-identifier <*unique-identifier*> **no client-identifier**	Specifies the unique ID of the user when binding an address manually
client-name <*name*> **no client-name**	Configures a client name when binding an address manually

3. Enable logging for address conflicts

Command	Explanation
Global Mode	
ip dhcp conflict logging **no ip dhcp conflict logging**	Enables logging for DHCP address to detect address conflicts
Admin Mode	
clear ip dhcp conflict <*address* | *all*>	Deletes a single address conflict record or all conflict records

14.2.2 DHCP Server Configuration Commands

14.2.2.1 bootfile

Command: bootfile <*filename*>

no bootfile

Function: Sets the file name for DHCP client to import on bootup; the "**no bootfile** " command deletes this setting.

Parameters: <*filename*> is the name of the file to be imported, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specify the name of the file to be imported for the client. This is usually used for diskless workstations that need to download a configuration file from the server on bootup. This command is together with the "next sever".

Example: The path and filename for the file to be imported is "c:\temp\nos.img"
Switch(dhcp-1-config)#bootfile c:\temp\nos.img

Related command: next-server

14.2.2.2 client-identifier

Command: client-identifier <*unique-identifier*>

no client-identifier

Function: Specifies the unique ID of the user when binding an address manually; the "**no client-identifier**" command deletes the identifier.

Parameters: <*unique-identifier*> is the user identifier, in dotted Hex format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with "host" when binding an address manually. If the requesting client identifier matches the specified identifier, DHCP server assigns

the IP address defined in "host" command to the client.

Example: Specifying the IP address 10.1.128.160 to be bound to user with the unique id of 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#client-identifier 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: host

14.2.2.3 client-name

Command: client-name <*name*>

no client-name

Function: Specifies the username when binding addresses manually; the "**no client-name**" command deletes the username.

Parameters: <*name*> is the name of the user, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Configure a username for the manual binding device, domain should not be included when configuring username.

Example: Giving the user, with unique id of 00-10-5a-60-af-12, a username of "network".

Switch(dhcp-1-config)#client-name network

14.2.2.4 default-router

Command: default-router <*address1*>[<*address2*>[…<*address8*>]]

no default-router

Function: Configures default gateway(s) for DHCP clients; the "**no default-router**" command deletes the default gateway.

Parameters: *address1…address8* are IP addresses, in decimal format.

Default: No default gateway is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: The IP address of default gateway(s) should be in the same subnet as the DHCP client IP, the switch supports up to 8 gateway addresses. The gateway address assigned first has the highest priority, and therefore address1 has the highest priority, and address2 has the second, and so on.

Example: Configuring the default gateway for DHCP clients to be 10.1.128.2 and 10.1.128.100.

Switch(dhcp-1-config)#default-router 10.1.128.2 10.1.128.100

14.2.2.5 dns-server

Command: dns-server <*address1*>[<*address2*>[…<*address8*>]]

no dns-server

Function: Configure DNS servers for DHCP clients; the "**no dns-server**" command deletes the default gateway.

Parameters: *address1…address8* are IP addresses, in decimal format.

Default: No DNS server is configured for DHCP clients by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: Up to 8 DNS server addresses can be configured. The DNS server address assigned first has the highest priority, Therefore address 1 has the highest priority, and address 2 has the second, and so on.

Example: Set 10.1.128.3 as the DNS server address for DHCP clients.

Switch(dhcp-1-config)#dns-server 10.1.128.3

14.2.2.6 domain-name

Command: domain-name <*domain*>

no domain-name

Function: Configures the Domain name for DHCP clients; the "**no domain-name**" command deletes the domain name.

Parameters: <*domain*> is the domain name, up to 255 characters are allowed.

Command Mode: DHCP Address Pool Mode

Usage Guide: Specifies a domain name for the client.

Example: Specifying "edgecore.com" as the DHCP clients' domain name.

Switch(dhcp-1-config)#domain-name edgecore.com

14.2.2.7 hardware-address

Command: hardware-address <*hardware-address*> [{Ethernet | IEEE802|<*type-number*>}]

no hardware-address

Function: Specifies the hardware address of the user when binding address manually; the "**no hardware-address**" command deletes the setting.

Parameters: <*hardware-address*> is the hardware address in Hex; **Ethernet | IEEE802** is the Ethernet protocol type, **<*type-number*>** should be the RFC number defined for protocol types, from 1 to 255, e.g., 0 for Ethernet and 6 for IEEE 802.

Default: The default protocol type is Ethernet,

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used with the "host" when binding address manually. If the requesting client hardware address matches the specified hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specify IP address 10.1.128.160 to be bound to the user with hardware address 00-00-e2-3a-26-04 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-00-e2-3a-26-04

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: host

14.2.2.8 host

Command: host <*address*> [<*mask*> | <*prefix-length*>]

no host

Function: Specifies the IP address to be assigned to the user when binding addresses manually; the "**no host**" command deletes the IP address.

Parameters: <***address***> is the IP address in decimal format; <***mask***> is the subnet mask in decimal format; <***prefix-length***> means mask is indicated by prefix. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30".

Command Mode: DHCP Address Pool Mode

Usage Guide: If no mask or prefix is configured when configuring the IP address, and no information in the IP address pool indicates anything about the mask, the system will assign a mask automatically according to the IP address class.

This command is used with "hardware address" command or "client identifier" command when binding addresses manually. If the identifier or hardware address of the requesting client matches the specified identifier or hardware address, the DHCP server assigns the IP address defined in "host" command to the client.

Example: Specifying IP address 10.1.128.160 to be bound to user with hardware address 00-10-5a-60-af-12 in manual address binding.

Switch(dhcp-1-config)#hardware-address 00-10-5a-60-af-12

Switch(dhcp-1-config)#host 10.1.128.160 24

Related command: hardware-address, client-identifier

14.2.2.9 ip dhcp conflict logging

Command: ip dhcp conflict logging

no ip dhcp conflict logging

Function: Enables logging for address conflicts detected by the DHCP server; the "**no ip dhcp conflict logging"** command disables the logging.

Default: Logging for address conflict is enabled by default.

Command mode: Global Mode

Usage Guide: When logging is enabled, once the address conflict is detected by the DHCP server, the conflicting address will be logged. Addresses present in the log for conflicts will not be assigned dynamically by the DHCP server until the conflicting records are deleted.

Example: Disable logging for DHCP server.
Switch(Config)#no ip dhcp conflict logging

Related command: clear ip dhcp conflict

14.2.2.10 ip dhcp excluded-address

Command: ip dhcp excluded-address <low-address>[<*high-address*>]

no ip dhcp excluded-address <low-address> [<high-address>]

Function: Specifies addresses excluding from dynamic assignment; the "**no ip dhcp excluded-address <*low-address*> [<*high-address*>]**" command cancels the setting.

Parameters: <***low-address***> is the starting IP address, **[<*high-address*>]** is the ending IP address.

Default: Only individual address is excluded by default.

Command mode: Global Mode

Usage Guide: This command can be used to exclude one or several consecutive addresses in the pool from being assigned dynamically so that those addresses can be used by the administrator for other purposes.

Example: Reserving addresses from 10.1.128.1 to 10.1.128.10 from dynamic assignment.

Switch(Config)#ip dhcp excluded-address 10.1.128.1 10.1.128.10

14.2.2.11 ip dhcp pool

Command: ip dhcp pool <*name*>

no ip dhcp pool <*name*>

Function: Configures a DHCP address pool and enter the pool mode; the "**no ip dhcp pool <*name*>"** command deletes the specified address pool.

Parameters: <*name*> is the address pool name, up to 255 characters are allowed.

Command mode: Global Mode

Usage Guide: This command is used to configure a DHCP address pool under Global Mode and enter the DHCP address configuration mode.

Example: Defining an address pool named "1".

Switch(Config)#ip dhcp pool 1

Switch(dhcp-1-config)#

14.2.2.12 loghost dhcp

Command: loghost dhcp <*ip-address*> <*port*>

no loghost dhcp

Function: Enables DHCP logging and specify the IP address and port number for the DHCP logging host; the "**no loghost dhcp"** command disables the DHCP logging function.

Parameters: <*ip-address*> is the DHCP log host IP address in decimal format. **<*port*>** is the port number, valid values range from 0 – 65535.

Default: DHCP logging is disabled by default.

Command mode: Global Mode

Usage Guide: The user can check information about DHCP address assignment from the log host when this command is configured. Any host running logtest.exe provided by Edge-Core can be a DHCP log host.

Example: Enabling the DHCP logging, the log host is 192.168.1.101, port 45.

Switch(Config)#loghost dhcp 192.168.1.101 45

14.2.2.13 lease

Command: lease { [<*days*>] [<*hours*>][<*minutes*>] | infinite }

no lease

Function: Sets the lease time for addresses in the address pool; the "**no lease**" command restores

the default setting.

Parameters: <***days***> is number of days from 0 to 365; <***hours*** is number of hours from 0 to 23; <***minutes***> is number of minutes from 0 to 59; **infinite** means perpetual use.

Default: The default lease duration is 1 day.

Command Mode: DHCP Address Pool Mode

Usage Guide: DHCP is the protocol to assign network addresses dynamically instead of permanently, hence the introduction of ease duration. Lease settings should be decided based on network conditions: too long lease duration offsets the flexibility of DHCP, while too short duration results in increased network traffic and overhead. The default lease duration of ES4704BD is 1 day.

Example: Setting the lease of DHCP pool "1" to 3 days 12 hours and 30 minutes.

Switch(dhcp-1-config)#lease 3 12 30

14.2.2.14 netbios-name-server

Command: netbios-name-server <*address1*>[<*address2*>[…<*address8*>]]

no netbios-name-server

Function: Configures WINS servers' address; the "**no netbios-name-server**" command deletes the WINS server.

Parameters: ***address1…address8*** are IP addresses, in decimal format.

Default: No WINS server is configured by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command is used to specify WINS server for the client, up to 8 WINS server addresses can be configured. The WINS server address assigned first has the highest priority. Therefore, address 1 has the highest priority, and address 2 the second, and so on.

14.2.2.15 netbios-node-type

Command: netbios-node-type {b-node|h-node|m-node|p-node|<*type-number*>}

no netbios-node-type

Function: Sets the node type for the specified port; the "**no netbios-node-type**" command cancels the setting.

Parameters: **b-node** stands for broadcasting node, **h-node** for hybrid node that broadcasts after point-to-point communication; **m-node** for hybrid node to communicate in point-to-point after broadcast; **p-node** for point-to-point node; <***type-number***> is the node type in Hex from 0 to FF.

Default: No client node type is specified by default.

Command Mode: DHCP Address Pool Mode

Usage Guide: If client node type is to be specified, it is recommended to set the client node type to **h-node** that broadcasts after point-to-point communication.

Example: Setting the node type for client of pool 1 to broadcasting node.

Switch(dhcp-1-config)#netbios-node-type b-node

14.2.2.16 network-address

Command: network-address <*network-number*> [<*mask*> | <*prefix-length*>]

no network-address

Function: Sets the scope for assignment for addresses in the pool; the "**no network-address**" command cancels the setting.

Parameters: <*network-number*> is the network number; **<*mask*>** is the subnet mask in the decimal format; **<*prefix-length*>** stands for mask in prefix form. For example, mask 255.255.255.0 in prefix is "24", and mask 255.255.255.252 in prefix is "30". Note: When using DHCP server, the pool mask should be longer or equal to that of layer 3 interface IP address in the corresponding segment.

Default: If no mask is specified, default mask will be assigned according to the address class.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command sets the scope of addresses that can be used for dynamic assignment by the DHCP server; one address pool can only have one corresponding segment. This command is exclusive with the manual address binding command "hardware address" and "host".

Example: Configuring the assignable address in pool 1 to be 10.1.128.0/24.

Switch(dhcp-1-config)#network-address 10.1.128.0 24

Related command: ip dhcp excluded-address

14.2.2.17 next-server

Command: next-server <*address1*>[<*address2*>[…<*address8*>]]

no next-server

Function: Sets the server address for storing the client import file; the "**no next-server**" command cancels the setting.

Parameters: *address1…address8* are IP addresses, in the decimal format.

Command Mode: DHCP Address Pool Mode

Usage Guide: This command configures the address for the server hosting client import file. This is usually used for diskless workstations that need to download configuration files from the server on bootup. This command is used together with "bootfile".

Example: Setting the hosting server address as 10.1.128.4.

Switch(dhcp-1-config)#next-server 10.1.128.4

Related command: bootfile

14.2.2.18 option

Command: option <*code*> {ascii <*string*> | hex <*hex*> | ipaddress <*ipaddress*>}

no option <*code*>

Function: Sets the network parameter specified by the option code; the "**no option <*code*>**" command cancels the setting for option.

Parameters: <*code*> is the code for network parameters; **<*string*>** is the ASCII string up to 255

characters; **<*hex*>** is a value in Hex that is no greater than 510 and must be of even length; **<*ipaddress*>** is the IP address in decimal format, up to 63 IP addresses can be configured.

Command Mode: DHCP Address Pool Mode

Usage Guide: The switch provides common commands for network parameter configuration as well as various commands useful in network configuration to meet different user needs. The definition of option code is described in detail in RFC2123.

Example: Setting the WWW server address as 10.1.128.240.

Switch(dhcp-1-config)#option 72 ip 10.1.128.240

14.2.2.19 service dhcp

Command: service dhcp

no service dhcp

Function: Enables DHCP server; the "**no service dhcp**" command disables the DHCP service.

Default: DHCP service is disabled by default.

Command mode: Global Mode

Usage Guide: Both DHCP server and DHCP relay are included in the DHCP service. When DHCP services are enabled, both DHCP server and DHCP relay are enabled. ES4704BD can only assign IP address for the DHCP clients and enable DHCP relay when DHCP server function is enabled.

Example: Enabling DHCP server.

Switch(Config)#service dhcp

14.3 DHCP Relay Configuration

When the DHCP client and server are in different segments, DHCP relay is required to transfer DHCP packets. Adding a DHCP relay makes it unnecessary to configure a DHCP server for each segment, one DHCP server can provide the network configuration parameter for clients from multiple segments, which is not only cost-effective but also management-effective.

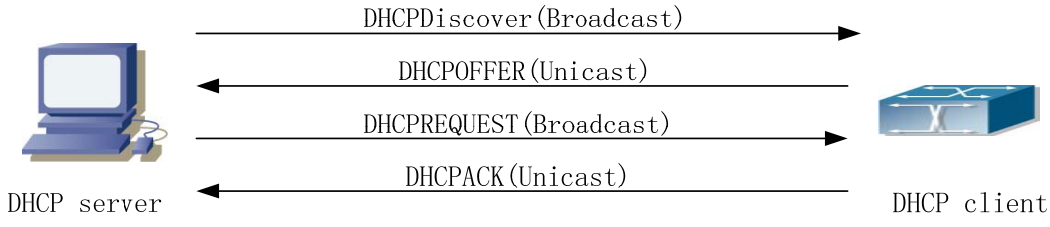


Fig 14-2 DHCP relay

As shown in the above figure, the DHCP client and the DHCP server are in different networks, the DHCP client performs the four DHCP steps as usual yet DHCP relay is added to the process.

1. The client broadcasts a DHCPDISCOVER packet, and DHCP relay inserts its own IP address to the relay agent field in the DHCPDISCOVER packet on receiving the packet, and forwards the packet to the specified DHCP server (for DHCP frame format, please refer to RFC2131).
2. On the receiving the DHCPDISCOVER packet forwarded by DHCP relay, the DHCP server sends the DHCPOFFER packet via DHCP relay to the DHCP client.
3. DHCP client chooses a DHCP server and broadcasts a DHCPREPLY packet, DHCP relay forwards the packet to the DHCP server after processing.
4. On receiving DHCPREPLY, the DHCP server responds with a DHCPACK packet via DHCP relay to the DHCP client.

DHCP relay can not only send DHCP broadcasting packets to the specified DHCP servers, but can also send other specified UDP broadcast packet to specified servers.

14.3.1 DHCP Relay Configuration Task Sequence

1. Enable DHCP relay.
2. Configure DHCP relay to forward DHCP broadcast packet.
3. Configure DHCP relay to forward other UDP broadcast packet.
4. Disable DHCP relay from forwarding DHCP broadcast packet.

1. Enable DHCP relay.

DHCP server and DHCP relay is enabled as the DHCP service.

2. Configure DHCP relay to forward DHCP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp <*port*> **no ip forward-protocol udp <*port*>**	The UDP port used for DHCP broadcast packet forwarding.
Interface Mode	
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	Sets the destination IP address for DHCP relay forwarding; the "**no ip helper-address <*ipaddress*>**" command cancels the setting.

3. Configure DHCP relay to forward other UDP broadcast packet.

Command	Explanation
Global Mode	
ip forward-protocol udp <*port*> **no ip forward-protocol udp <*port*>**	Specifies the DHCP relay forwarding protocol by setting UDP port; the "**no ip forward-protocol udp <*port*>**" command cancels the setting.
ip helper-address <*ipaddress*> **no ip helper-address <*ipaddress*>**	Sets the destination IP address for DHCP relay forwarding; the "**no ip helper-address <*ipaddress*>**" command cancels the setting.

4. Disable DHCP relay from forwarding DHCP broadcast packet.

Command	Explanation
Global Mode	

ip dhcp relay information policy drop **no ip dhcp relay information policy drop**	When layer 3 switches are used as DHCP relays, this command sets the relay forwarding policy to drop DHCP packets; the "**no ip dhcp relay information policy drop**" command allows DHCP packets forwarding.

14.3.2 DHCP Relay Configuration Command

14.3.2.1 ip forward-protocol udp

Command: ip forward-protocol udp <port>

no ip forward-protocol udp <port>

Function: Sets DHCP relay to forward UPD broadcast packets on the port; the "**no ip forward-protocol udp <port>**" command cancels the service.

Default: DHCP relay forwards DHCP broadcast packet to UDP port 67 by default.

Command mode: Global Mode

Usage Guide: The forwarding destination address is set in the "**ip helper-address**" command and described later.

Example: Setting TFTP packets to be forwarded to 192.168.1.5.

Switch(Config)#ip forward-protocol udp 69

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip helper-address 192.168.1.5

14.3.2.2 ip helper-address

Command: ip helper-address <*ip-address*>

no ip helper-address <*ip-address*>

Function: Specifies the destination address for the DHCP relay to forward UDP packets. The "**no ip helper-address <*ip-address*>**" command cancels the setting.

Default: Address for forwarding DHCP broadcast packet is set on DHCP relay by default.

Command mode: Interface Mode

Usage Guide: The DHCP relay forwarding server address corresponds to the port forwarding UDP, i.e., DHCP relay forwards corresponding UDP packets only to the corresponding server instead of all UDP packets to all servers. The default setting of DHCP relay is to forward DHCP packets on UDP port 67 to the DHCP server. When this command is run after "**ip forward-protocol udp <*port*>**" command, the forwarding address configured by this command receives the UDP packets from **<*port*>** instead of default DHCP packets. If a different set of UDP forwarding protocol and receiving server address is to be set, the combination of "**ip forward-protocol udp <*port*>**" command and this command should be used for configuration.

14.3.2.3 ip dhcp relay information policy drop

Command: ip dhcp relay information policy drop

no ip dhcp relay information policy drop

Function: When layer 3 switches are used as DHCP relays, this command sets the relay forwarding policy to drop DHCP packets; the "**no ip dhcp relay information policy drop**" command allows DHCP packets forwarding.

Default: DHCP relay forwards DHCP broadcast packet by default.

Command mode: Global Mode

Usage Guide: When the DHCP relay should not forward DHCP packets for some reason, this command can be used to disable DHCP packet forwarding on DHCP relay.

Example: Disabling DHCP broadcast packet forwarding on the layer 3 switch.

Switch(Config)# ip dhcp relay information policy drop

14.4 DHCP Configuration Example

Scenario 1:

Too save configuration efforts of network administrators and users a company is using ES4704BD as a DHCP server. The Admin VLAN IP address is 10.16.1.2/16. The local area network for the company is divided into network A and B according to the office locations. The network configurations for location A and B are shown below.

PoolA(network 10.16.1.0)		PoolB(network 10.16.2.0)	
Device	IP address	Device	IP address
Default gateway	10.16.1.200 10.16.1.201	Default gateway	10.16.1.200 10.16.1.201
DNS server	10.16.1.202	DNS server	10.16.1.202
WINS server	10.16.1.209	WINS server	10.16.1.209
WINS node type	H-node	WINS node type	H-node
Lease	3 days	Lease	3 days

In location A, a machine with MAC address 00-03-22-23-dc-ab is assigned with a fixed IP address of 10.16.1.210 and named as "management". (The interfaces in the following configurations are wrong; "no switch" command is not available.)

Switch(Config)#service dhcp

Switch(Config)#interface vlan 1

Switch(Config-Vlan-1)#ip address 10.16.1.2 255.255.0.0

Switch(Config-Vlan-1)#exit

Switch(Config)#ip dhcp pool A

Switch(dhcp-A-config)#network 10.16.1.0 24

Switch(dhcp-A-config)#lease 3

Switch(dhcp-A-config)#default-route 10.16.1.200 10.16.1.201

Switch(dhcp-A-config)#dns-server 10.16.1.202

Switch(dhcp-A-config)#netbios-name-server 10.16.1.209

Switch(dhcp-A-config)#netbios-node-type H-node

Switch(dhcp-A-config)#exit

Switch(Config)#ip dhcp excluded-address 10.16.1.200 10.16.1.210

Switch(Config)#ip dhcp pool B

Switch(dhcp-B-config)#network 10.16.2.0 24

Switch(dhcp-B-config)#lease 1

Switch(dhcp-B-config)#default-route 10.16.2.200 10.16.2.201

Switch(dhcp-B-config)#dns-server 10.16.2.202

Switch(dhcp-B-config)#option 72 ip 10.16.2.209

Switch(dhcp-config)#exit

Switch(Config)#ip dhcp excluded-address 10.16.2.200 10.16.2.210

Switch(Config)#ip dhcp pool A1

Switch(dhcp-A1-config)#host 10.16.1.210

Switch(dhcp-A1-config)#hardware-address 00-03-22-23-dc-ab

Switch(dhcp-A1-config)# client-name management

Switch(dhcp-A1-config)#exit

Scenario 2:

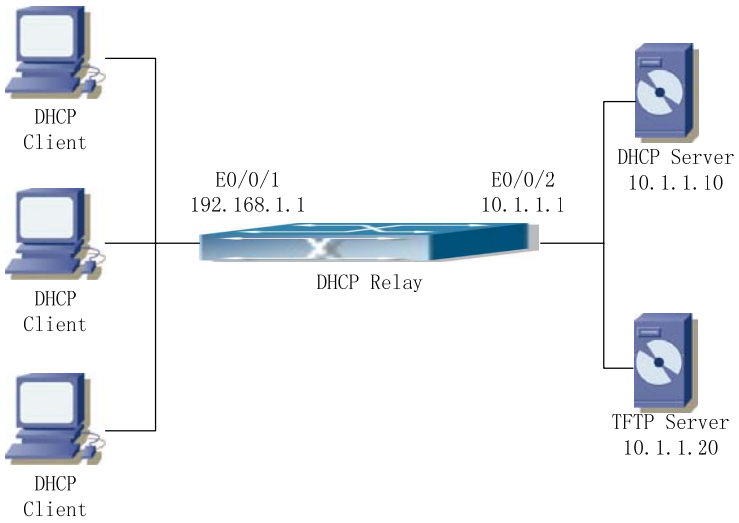


Fig 14-3 DHCP Relay Configuration

As shown in the above figure, ES4704BD is configured as a DHCP relay. The DHCP server address is 10.1.1.10, TFTP server address is 10.1.1.20, the configuration steps are as follows:

Switch(Config)# service dhcp

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip address 192.168.1.1 255.255.255.0

Switch(Config-If-Vlan1)#exit

Switch(Config)#interface vlan 2

Switch(Config-If-Vlan2)#ip address 10.1.1.1 255.255.255.0

Switch(Config-If-Vlan2)#exit

Switch(Config)#ip forward-protocol udp 67

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip help-address 10.1.1.10

Switch(Config-If-Vlan1)#exit

Switch(Config)#ip forward-protocol udp 69

Switch(Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip help-address 10.1.1.20

Note: DHCP server address and TFTP server address must be configured separately since their receiving UDP protocols are different. It is recommended to use the combination of command "**ip forward-protocol udp <*port*>**" and "**ip helper-address <*ipaddress*>**". "**ip help-address**" can only be configured for ports on layer 3 and cannot be configured on layer 2 ports directly.

Usage Guide:

When a DHCP/BootP client is connected to a VLAN1 port of the switch, the client can only get its address from 10.16.1.0/24 instead of 10.16.2.0/24. This is because the broadcast packet from the

client will be requesting the IP address in the same segment of the VLAN interface after VLAN interface forwarding, and the VLAN interface IP address is 10.16.1.2/24, therefore the IP address assigned to the client will belong to 10.16.1.0/24.

If the DHCP/BootP client wants to have an address in 10.16.2.0/24, the gateway forwarding broadcast packets of the client must belong to 10.16.2.0/24. The connectivity between the client gateway and the switch must be ensured for the client to get an IP address from the 10.16.2.0/24 address pool.

14.5 DHCP Troubleshooting Help

14.5.1 Monitor and Debug Commands

14.5.1.1 clear ip dhcp binding

Command: clear ip dhcp binding {<*address*> | all }

Function: Deletes the specified IP address-hardware address binding record or all IP address-hardware address binding records.

Parameters: <*address*> is the IP address that has a binding record in decimal format. **all** refers to all IP addresses that have a binding record.

Command mode: Admin Mode

Usage Guide: "**show ip dhcp binding**" command can be used to view binding information for IP addresses and corresponding DHCP client hardware addresses. If the DHCP server is informed that a DHCP client is not using the assigned IP address for some reason before the lease period expires, the DHCP server would not remove the binding information automatically. The system administrator can use this command to delete that IP address-client hardware address binding manually, if "all" is specified, then all auto binding records will be deleted, thus all addresses in the DHCP address pool will be reallocated.

Example: Removing all IP-hardware address binding records.

Switch#clear ip dhcp binding all

Related command: show ip dhcp binding

14.5.1.2 clear ip dhcp conflict

Command: clear ip dhcp conflict {<*address*> | all }

Function: Deletes an address present in the address conflict log.

Parameters: <*address*> is the IP address that has a conflict record; **all** stands for all addresses that have conflict records.

Command mode: Admin Mode

Usage Guide: "**show ip dhcp conflict**" command can be used to check which IP addresses are

conflicting for use. The **"Clear ip dhcp conflict"** command can be used to delete the conflict record for an address. If "all" is specified, then all conflict records in the log will be removed. When records are removed from the log, the addresses are available for allocation by the DHCP server.

Example: The network administrator finds 10.1.128.160 that has a conflict record in the log and is no longer used by anyone, so he deletes the record from the address conflict log.

Switch#clear ip dhcp conflict 10.1.128.160

Related command: ip dhcp conflict logging，show ip dhcp conflict

14.5.1.3 clear ip dhcp server statistics

Command: clear ip dhcp server statistics

Function: Deletes the statistics for DHCP server, clears the DHCP server count.

Command mode: Admin Mode

Usage Guide: DHCP count statistics can be viewed with "**show ip dhcp server statistics**" command, all information is accumulated. You can use the "**clear ip dhcp server statistics**" command to clear the count for easier statistics checking.

Example: clearing the count for DHCP server.

Switch#clear ip dhcp server statistics

Related command: show ip dhcp server statistics

14.5.1.4 show ip dhcp binding

Command: show ip dhcp binding [[<*ip-addr*>] + [type {all | manual | dynamic}] [count]]

Function: Displays IP-MAC binding information.

Parameters: <*ip-addr*> is a specified IP address in decimal format; "all" stands for all binding types (manual binding and dynamic assignment); "manual" for manual binding; "dynamic" for dynamic assignment; "count" displays statistics for DHCP address binding entries.

Command mode: Admin Mode

Example:

Switch# show ip dhcp binding

IP address	Hardware address	Lease expiration	Type
10.1.1.233	00-00-E2-3A-26-04	Infinite	Manual
10.1.1.254	00-00-E2-3A-5C-D3	60	Automatic

Displayed information	Explanation
IP address	IP address assigned to a DHCP client
Hardware address	MAC address of a DHCP client
Lease expiration	Valid time for the DHCP client to hold the IP address

Type	Type of assignment: manual binding or dynamic assignment.

14.5.1.5 show ip dhcp conflict

Command: show ip dhcp conflict

Function: Displays log information for addresses that have a conflict record.

Command mode: Admin Mode

Example:

Switch# show ip dhcp conflict

IP Address Detection method Detection Time

10.1.1.1 Ping FRI JAN 02 00:07:01 2002

Displayed information	Explanation
IP Address	Conflicting IP address
Detection method	Method in which the conflict is detected.
Detection Time	Time when the conflict is detected.

14.5.1.6 show ip dhcp server statistics

Command: show ip dhcp server statistics

Function: Displays statistics of all DHCP packets for a DHCP server.

Command mode: Admin Mode

Example:

Switch# show ip dhcp server statistics

Address pools 3

Database agents 0

Automatic bindings 2

Manual bindings 0

Conflict bindings 0

Expired bindings 0

Malformed message 0

Message Received

BOOTREQUEST 3814

DHCPDISCOVER 1899

DHCPREQUEST 6

DHCPDECLINE 0

DHCPRELEASE 1

DHCPINFORM 1

Message Send

BOOTREPLY 1911
DHCPOFFER 6
DHCPACK 6
DHCPNAK 0
DHCPRELAY 1907
DHCPFORWARD 0
Switch#

Displayed information	Explanation
Address pools	Number of DHCP address pools configured.
Database agents	Number of database agents.
Automatic bindings	Number of addresses assigned automatically
Manual bindings	Number of addresses bound manually
Conflict bindings	Number of conflicting addresses
Expired bindings	Number of addresses whose leases are expired
Malformed message	Number of error messages.
Message Received	Statistics for DHCP packets received
BOOTREQUEST	Total packets received
DHCPDISCOVER	Number of DHCPDISCOVER packets
DHCPREQUEST	Number of DHCPREQUEST packets
DHCPDECLINE	Number of DHCPDECLINE packets
DHCPRELEASE	Number of DHCPRELEASE packets
DHCPINFORM	Number of DHCPINFORM packets
Message Send	Statistics for DHCP packets sent
BOOTREPLY	Total packets sent
DHCPOFFER	Number of DHCPOFFER packets
DHCPACK	Number of DHCPACK packets
DHCPNAK	Number of DHCPNAK packets
DHCPRELAY	Number of DHCPRELAY packets
DHCPFORWARD	Number of DHCPFORWARD packets

14.5.1.7 debug ip dhcp server

Command: debug ip dhcp server { events|linkage|packets }

no debug ip dhcp server { events|linkage|packets }

Function: Enables DHCP server debug information: the "**no debug ip dhcp server { events|linkage|packets }"** command disables the debug information for DHCP server**.**

Default: Debug information is disabled by default.

Command mode: Admin Mode

14.5.2 DHCP Troubleshooting Help

If the DHCP clients cannot obtain IP addresses and other network parameters, the following procedures can be followed after DHCP client hardware and cables have been verified to be ok.

- ☞ Verify the DHCP server is running, start the related DHCP server if not running.
- ☞ If the DHCP clients and servers are not in the same physical network, verify that the router responsible for DHCP packet forwarding has DHCP relay function. If DHCP relay is not available for the intermediate router, it is recommended to replace the router or upgrade its software to one that has a DHCP relay function.
- ☞ In such case, the DHCP server should be examined for an address pool that is in the same segment of the switch VLAN, such a pool should be added if not present. (This does not indicate ES4704BD cannot assign IP address for different segments, see solution 2 for details.)
- ☞ If in DHCP service, pools for dynamic IP allocation and manual binding are conflicting, i.e., if command "**network-address**" and "**host**" are run for a pool, then only one of them will take effect; furthermore, in manual binding, only one IP-MAC binding can be configured in a pool. If multiple bindings are required, multiple manual pools can be created and IP-MAC bindings set for each pool. New configuration in the same pool will overwrite the previous configuration.

14.6 Web management

14.6.1 DHCP server configuration

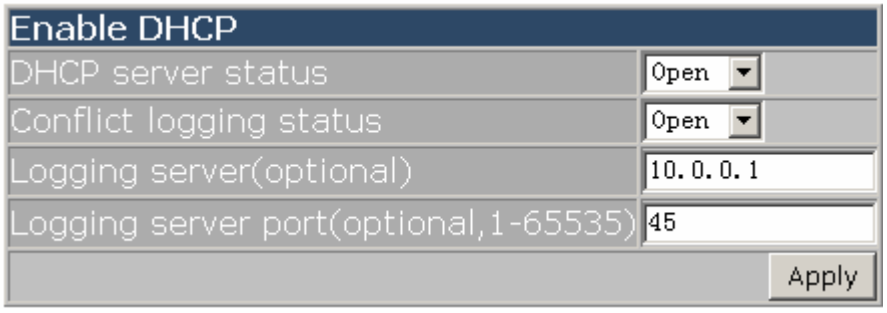
Click "DHCP configuration", to open switch DHCP function configuration management list. User may make switch DHCP function configurations

14.6.2 Enable DHCP

Click "DHCP configuration", "DHCP server configuration", Enable DHCP. You may configure enable or disable the DHCP server, configure address collision log server function, and more

- DHCP server status - enables, disables the DHCP server function. This is the same as CLI command 14.2.2.19)
- Conflict logging status - enables, disables the DHCP server checking address conflict log function. This is the same as CLI command 14.2.2.9
- Logging server(optional) – assign a DHCP logging server IP address. This is the same as CLI command 14.2.2.12
- Logging server port (optional,1-65535) – assign a DHCP logging server port ID

Example: Choose DHCP server status as open, choose Conflict logging status as open, configure Logging server as 10.0.0.1, configure Logging server port as 45, click Apply button, to apply the configuration to switch..

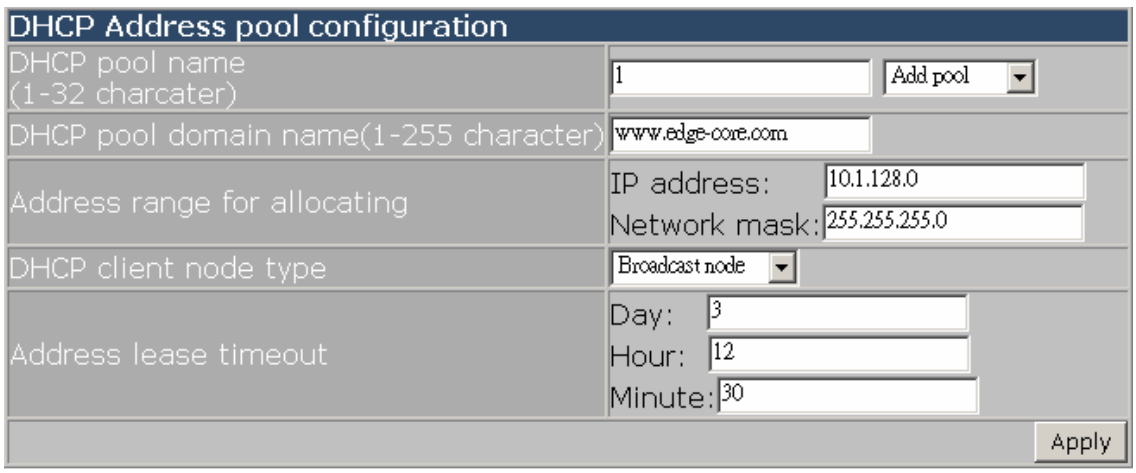


14.6.2.1 Address pool configuration

Click "DHCP configuration", "DHCP server configuration", "Address pool configuration" to configure the DHCP address pool function:

- DHCP pool name (1-32 characters) – defines a DHCP address pool in global mode. Same as CLI command 14.2.2.11
- DHCP pool domain name (1-255 characters) – to configure DHCP client domain name. Same as CLI command 14.2.2.6
- Address range for allocating – Configures a specific address range for the address pool. Same as CLI command 14.2.2.16
- DHCP client node type – Configures the DHCP client node type: broadcast node is broadcast type; Hybrid node is first peer-to-peer then broadcast mixed type; Mixed node is first broadcast then peer-to-peer; Peer-to-peer node is peer-to-peer type. Same as CLI command 14.2.2.15
- Address lease timeout – Configures the address lease timeout in address pool, where "0" means everlasting use. Same as CLI command 14.2.2.13

Example: Configure DHCP pool name as 1, DHCP pool domain name as www.edge-core.com, the Address range for allocating IP addresses as10.1.128.0, Network mask as 255.255.255.0, DHCP client node type as broadcast node, Address lease timeout as 3 days 12 hours 30 minute ,and lastly, click the Apply button to apply the configuration to the switch.

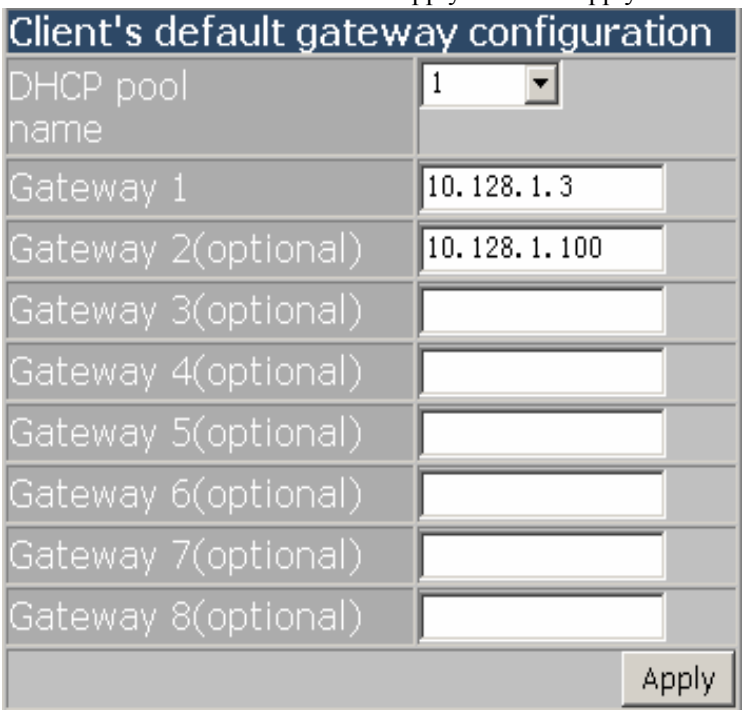


14.6.2.2 Client's default gateway configuration

Click "DHCP configuration", "DHCP server configuration", "Client's default gateway configuration" to configure the default gateway for DHCP client. Same as CLI command 14.2.2.4:

- DHCP pool name – selects one DHCP address pool
- Gateway – default gateway, default gateway's IP address and DHCP client's IP address in the same segment. The switch maximum supports 8 gateway addresses. The headmost configured gateway address, or address 1, has the highest priority, then address2, address3, etc.

Example: Select DHCP pool name as 1, configure Gateway 1 as 10.128.1. 3, configure Gateway 2 as 10.128.1.100 and then click the Apply button to apply this configuration to the switch.

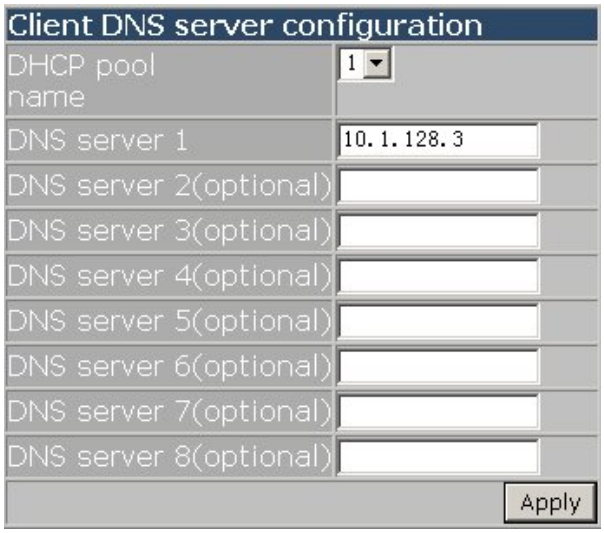


14.6.2.3 Client dns server configuration

Click "DHCP configuration", "DHCP server configuration", "Client DNS server configuration" to configure the DNS server for the DHCP client. Same as CLI command 14.2.2.5:

- DHCP pool name – choose one DHCP address pool
- DNS server – DNS server. The system maximum supports 8 DNS server addresses. The headmost configured DNS server address, address1, has the highest priority, then address2, address3, etc.

Example: Choose DHCP pool name as 1. Configure DNS server 1 as 10.1.128.3. Click the Apply button to apply this configuration to switch.

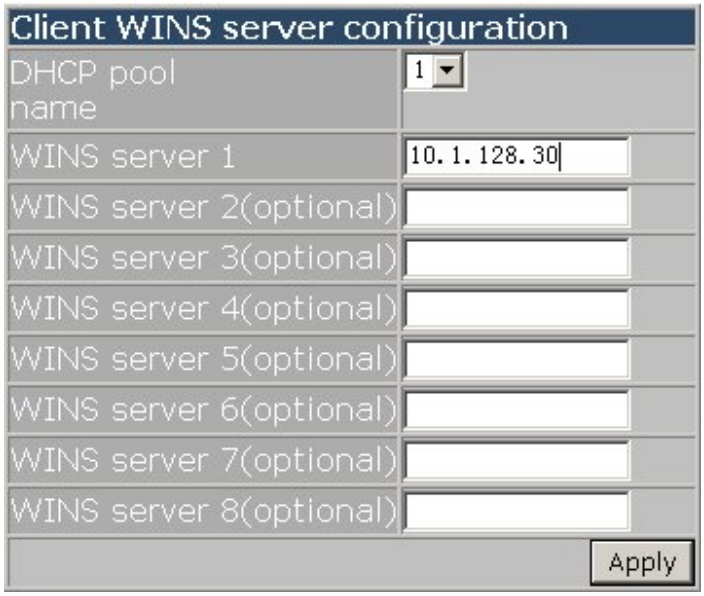


14.6.2.4 Client wins server configuration

Click DHCP configuration, DHCP server configuration, Client WINS server configuration. Configure Wins server address. Same as CLI command 14.2.2.14:

- DHCP pool name – choose one DHCP address pool
- WINS server – WINS server, system maximum support configure 8 WINS server address, the headmost configured WINS server address has the higher priority, so the address1 has the highest priority, then address2, address3 in turn

Choose DHCP pool name as 1, configure WINS server 1 as 10.1.128.30. Click Apply button to apply this configuration to switch.

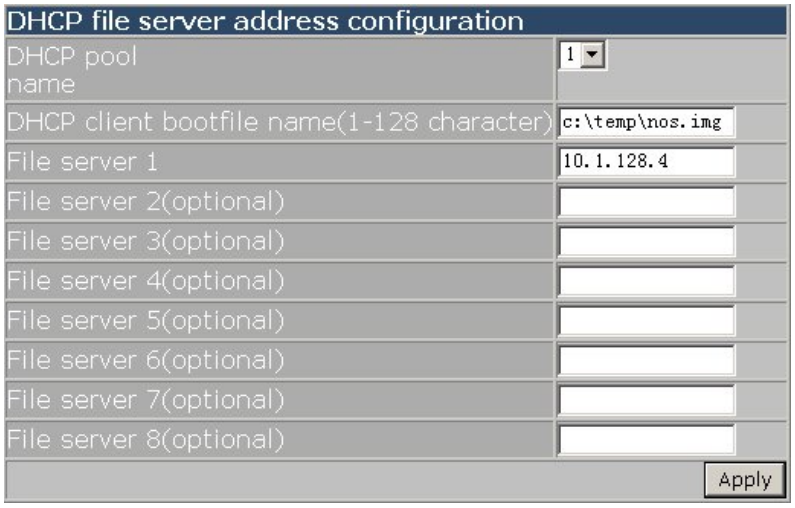


14.6.2.5 DHCP file server address configuration

Click “DHCP configuration”, “DHCP server configuration”, “DHCP file server address configuration” to configure the DHCP client boot file name and client server address which is for save the boot file:

- DHCP pool name - Choose one DHCP address pool
- DHCP client bootfile name (1-128 characters) - boot file name. Same as CLI command 14.2.2.1
- File server - server address where the client boot file is saved. Same as CLI command 14.2.2.17

Example: Choose DHCP pool name as 1, configure the DHCP client bootfile name as c:\temp\nos.img, configure File server1 as 10.1.128.4, and then, click the Apply button to apply this configuration to switch.

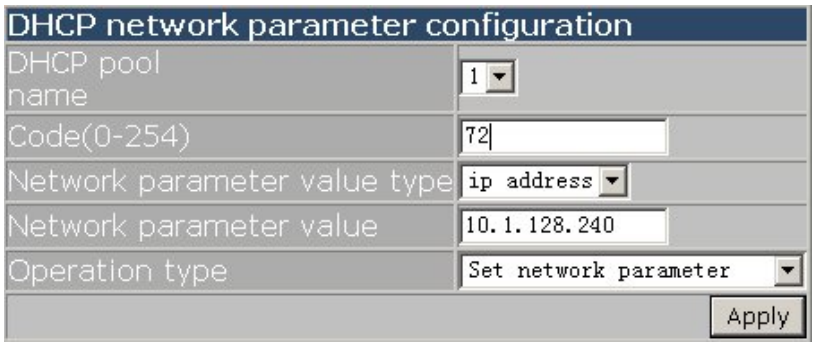


14.6.2.6 DHCP network parameter configuration

Click “DHCP configuration”, “DHCP server configuration”, “DHCP network parameter configuration” to specify network parameters. Same as CLI command 14.2.2.18:

- DHCP pool name - Choose one DHCP address pool
- Code (0-254) - network parameter code
- Network parameter value type – configures network parameter type. Ascii is an ASCII string with maximum of 255 characters; hex is hex number with maximum of 510. Length must be an even number. ip address is IP address
- Network parameter value – parameter value
- Operation type – configures or cancels network parameter

Example: Choose DHCP pool name as 1, configure Code as 72, choose Network parameter value type as IP address, configure Network parameter value as 10.1.128.240, choose Operation type as Set network parameter, and then click the Apply button to apply this configuration to switch.

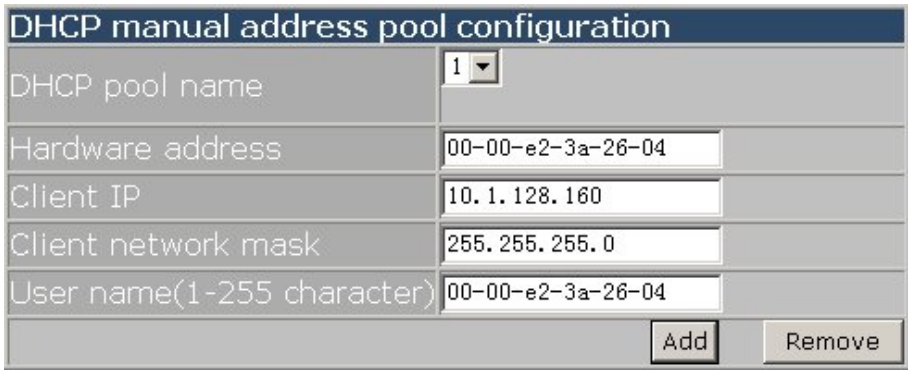


14.6.2.7 Manual address pool configuration

Click "DHCP configuration", "DHCP server configuration", "Manual address pool configuration" to configure DHCP to manually allocate address:

- DHCP pool name – Choose one DHCP address pool
- Hardware address – assigns user hardware address. Same as CLI command 14.2.2.7
- Client IP – allocated IP address for a specific client
- Client network mask – allocated IP address mask for a specific client. Same as CLI command 14.2.2.8
- User name (1-255 characters) – assigns user exclusive name. Same as CLI command 14.2.2.2

Example: Choose DHCP pool name as 1, configure Hardware address as 00-00-e2-3a-26-04, configure Client IP as 10.1.128.160, configure Client network mask as 255.255.255.0, configure User name as 00-00-e2-3a-26-04, and then click Add to apply the configuration to switch.

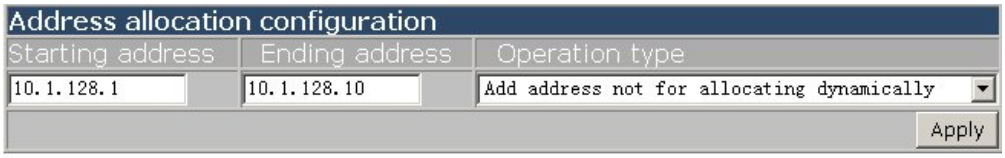


14.6.2.8 Excluded address configuration

Click "DHCP configuration", "DHCP server configuration", "Excluded address configuration" to exclude an address from dynamic allocation in the address pool. Same as CLI command 14.2.2.10:

- Starting address – is starting IP address
- Ending address – is ending IP address
- Operation type – configures or removes the address which will not be dynamic allocated in the address pool.

Example: Configure the Starting address as 10.1.128.1, configure Ending address as 10.1.128.10, and choose Operation type as Add address not for allocating dynamically. Click Apply button to apply this configuration to switch.



Address allocation configuration		
Starting address	Ending address	Operation type
10.1.128.1	10.1.128.10	Add address not for allocating dynamically
		Apply

Address list	
Starting address	Ending address
10.1.128.1	10.1.128.10
end of list	

14.6.2.9 DHCP packet statistics

Click “DHCP configuration”, “DHCP server configuration”, “DHCP packet statistics” to display DHCP server statistics information of all kinds of DHCP data packets. Same as CLI command 14.5.1.3:

DHCP packet statistics	
Memory usage rate	96
Address pool	1
Proxy database	0
Dynamical allocated address	0
Manual binded address	0
Address conflict	0
Binding exceeding lease time	0
Errors	0
Received DHCP packet statistics	
Received	0
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Transmitted DHCP packet statistics	
Transmitted	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0
DHCPRELAY	0
DHCPFORWARD	0

14.6.3 DHCP relay configuration

Click “DHCP configuration”, “DHCP server configuration”, “DHCP packet statistics” to display DHCP server statistics information for all kinds of DHCP data packets. Same as CLI command 14.5.1.3:

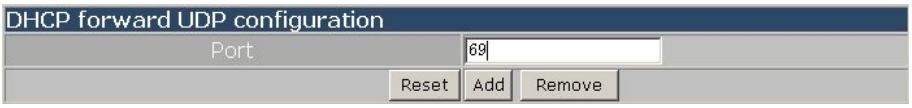
14.6.3.1 DHCP relay configuration

Click “DHCP configuration”, “DHCP relay configuration”, “DHCP relay configuration” to configure the switch’s DHCP relay function:

DHCP forward UDP configuration configures DHCP relay to forward broadcast messages to a UDP port. Same as CLI command 14.3.2.1:

- Port - UDP port

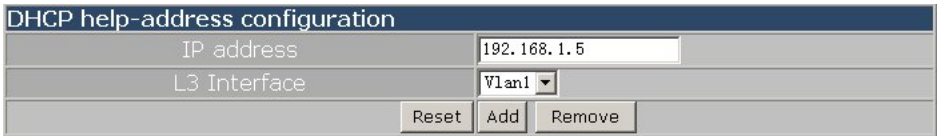
Example: Configure Port as 69, and then click Add button to apply this configuration to switch.



DHCP help-address configuration assigns a destination address to where DHCP relay forwards UDP messages. Same as CLI command 14.3.2.2:

- IP address – server address
- L3 Interface – Layer 3 port

Example: Configure IP address as 192.168.1.5, choose L3 Interface as Vlan1 Click Add button, to apply this configuration to switch.



When layer 3 switch is working as DHCP relay, to configure the relay forwarding policy as non-forwarding DHCP messages, click the Apply button. This will close the switch’s DHCP forwarding function. Click the Reset button to enable the switch’s DHCP forwarding function. The Default button restores the switch to forwarding DHCP in default mode.

14.6.4 DHCP debugging

Click “DHCP configuration”, “DHCP debugging”, to enable the switch DHCP debugging function list to display switch DHCP configuration and debugging information.

14.6.4.1 Delete binding log

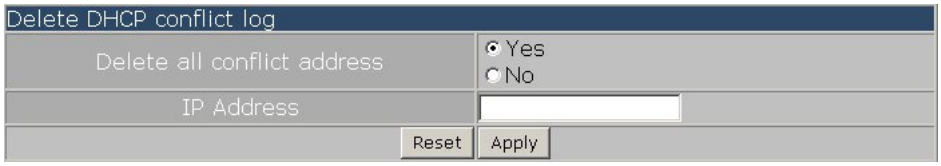
Click ”DHCP configuration”, ”DHCP debugging”, ”Delete binding log” to remove some specific IP address, the hardware address binding log or all IP addresses with relevant hardware address binding logs.

Example: Choose Delete all binding log as Yes then click Apply button to remove all IP addresses and hardware address binding records.

14.6.4.2 Delete conflict log

Click “DHCP configuration”, “DHCP debugging” to delete conflicting logs.

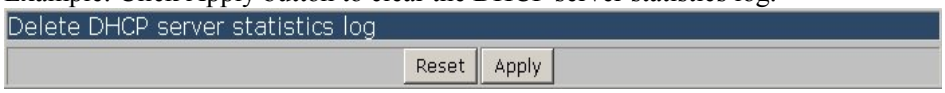
Example: Choose Delete all conflict address as Yes. Click Apply button and all conflicting addresses in address conflict log will be removed.



14.6.4.3 Delete DHCP server statistics log

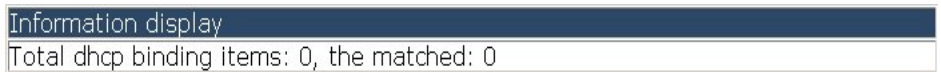
Click “DHCP configuration”, “DHCP debugging”, “Delete DHCP server statistics log”. Deletes the DHCP server statistics log to make DHCP server tally clear.

Example: Click Apply button to clear the DHCP server statistics log.



14.6.4.4 Show IP-Mac binding

Click “DHCP configuration”, “DHCP debugging”, “Show IP-MAC binding” to display IP address and MAC address binding situation.



14.6.2.5 Show conflict-logging

Click “DHCP configuration”, “DHCP debugging”, “Show conflict-logging” to display log information of which address has a conflict log.

Chapter 15 SNTP Configuration

The Network Time Protocol (NTP) is widely used for clock synchronization for global computers connected to the Internet. NTP can assess packet sending/receiving delay in the network, and estimate the computer's clock deviation independently, so as to achieve high accuracy in network computer clocking. In most positions, NTP can provide accuracy from 1 to 50ms according to the characteristics of the synchronization source and network route.

Simple Network Time Protocol (SNTP) is the simplified version of NTP, removing the complex algorithm of NTP. SNTP is used for hosts who do not require full NTP functions, it is a subset of NTP. It is common practice to synchronize the clocks of several hosts in local area network with other NTP hosts through the Internet, and use those hosts to provide time synchronization service for other clients in LAN. The figure below (Fig 15-1) depicts a NTP/SNTP application network topology, where SNTP mainly works between second level servers and various terminals since such scenarios do not require very high time accuracy, and the accuracy of SNTP (1 to 50 ms) is usually sufficient for those services.

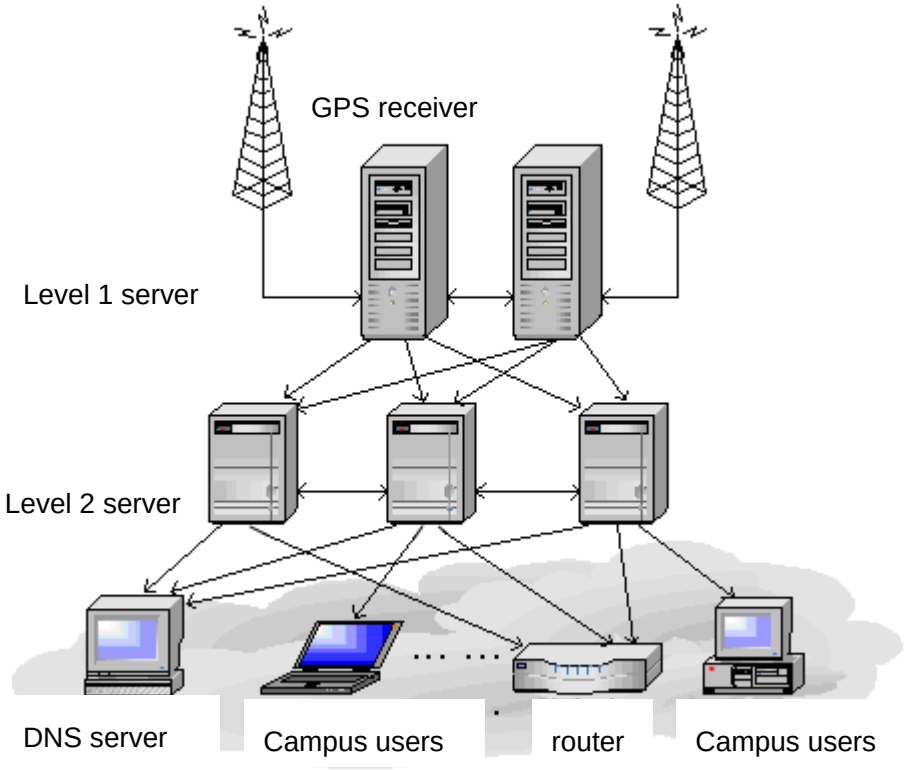


Fig 15-1 Working Scenario

ES4704BD implements SNTPv4 and supports SNTP client unicast as described in RFC2030; SNTP client multicast and unicast are not supported, nor is the SNTP server function.

15.1 SNTP Configuration Commands

15.1.1 sntp server

Command: sntp server <*server_address*> [version <*version_no*>]

no sntp server <*server_address*>

Function: Sets the SNTP/NTP server address and server version; the "**no sntp server <*server_address*>**" command deletes the SNTP/NTP server address.

Parameters: **<*server-address*>** is the IP unicast address of SNTP/NTP server, in decimal format; **<*version_no*>** is the client SNTP version number, valid values are 1 – 4. Default version number is 1.

Default: This setting is not configured upon switch shipment.

Command mode: Global Mode

Example: Setting a SNTP/NTP server address.

Switch(Config)#sntp server 10.1.1.1 version 4

15.1.2 sntp polltime

Command: sntp polltime <*interval*>

no sntp polltime

Function: Sets the interval for SNTP clients to send requests to NTP/SNTP; the "**no sntp polltime**" command cancels the polltime sets and restores the default setting.

Parameters: **< *interval*>** is the interval value from 16 to 16284.

Default: The default polltime is 64 seconds.

Command mode: Global Mode

Example: Setting the client to send request to the server every 128 seconds.

Switch#config

Switch(Config)#sntp polltime 128

15.1.3 sntp timezone

Command: sntp timezone <*name*> *{add | subtract}* <*time_difference*>

no sntp timezone

Function: Sets the time difference between the time zone in which the SNTP client resides and UTC. The "**no sntp timezone**" command cancels the time zone set and restores the default setting.

Parameters: **<*name*>** is the time zone name, up to 16 characters are allowed; **<*add*>** means the time zone equals UTC time plus **<*time_difference*>**; **<*subtract*>** means the time zone equals UTC time minus **<*time_difference*>**; **<*time_difference*>** is the time difference, from 1 to 12.

Default: The default time difference setting is “add 8”.

Command mode: Global Mode

Example: Setting the time zone to Beijing.

Switch#config
Switch(Config)#sntp timezone beijing add 8

15.2 Typical SNTP Configuration Examples

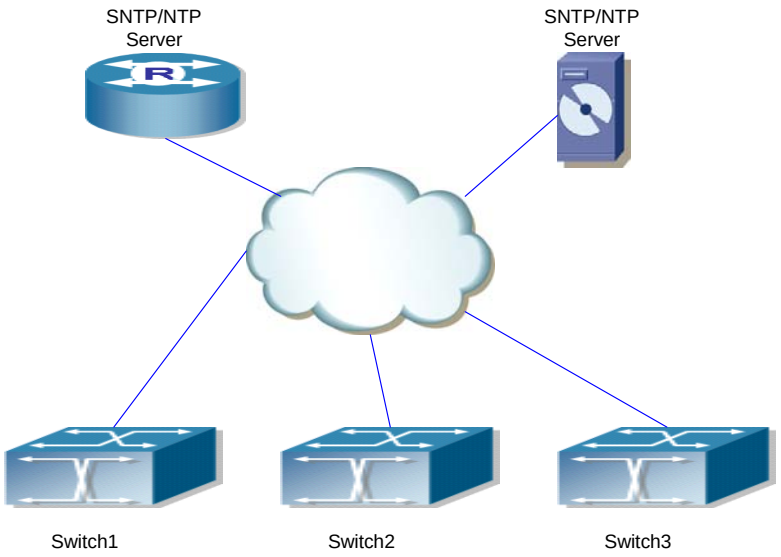


Fig 15-2 Typical SNTP Configuration

All ES4704BD switches in the autonomous zone are required to perform time synchronization, which is done through two redundant SNTP/NTP servers. For time to be synchronized, the network must be properly configured. There should be reachable route between any ES4704BD and the two SNTP/NTP servers.

Example: Assume the IP addresses of the SNTP/NTP servers are 10.1.1.1 and 20.1.1.1, respectively, and SNTP/NTP server function (such as NTP master) is enabled, then configurations for any ES4704BD should like the following:

Switch#config

Switch (Config)#sntp server 10.1.1.1

Switch (Config)#sntp server 20.1.1.1

From now on, SNTP would perform time synchronization to the server according to the default setting (polltime 64s, version 1).

15.3 SNTP Troubleshooting Help

15.3.1 Monitor and Debug Commands

15.3.1.1 show sntp

Command: show sntp

Function: Displays current SNTP client configuration and server status.

Parameters: N/A.

Command mode: Admin Mode

Example: Displaying current SNTP configuration.

Switch#show sntp

SNTP server	Version	Last Receive
2.1.0.2	1	never

15.3.1.2 debug sntp

Command: debug sntp {adjust | packets | select }

no debug sntp {adjust | packets | select}

Function: Displays or disables SNTP debug information.

Parameters: adjust stands for SNTP clock adjustment information; **packet** for SNTP packets, **select** for SNTP clock selection.

Command mode: Admin Mode

Example: Displaying debugging information for SNTP packets.

Switch#debug sntp packets

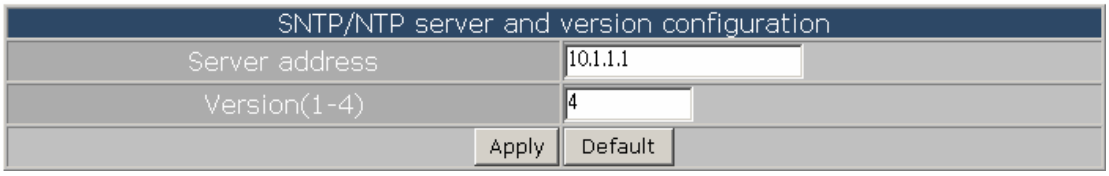
15.4 WEB MANAGEMENT

Click “SNTP configuration” to open the switch SNTP configuration management list. Users may then make configuration to switch’s SNTP settings.

15.4.1 SNMP/NTP server configuration

Click “SNTP configuration”, “SNTP/NTP server configuration” to configure SNTP/NTP server address and server version. Same as CLI command 15.1.1

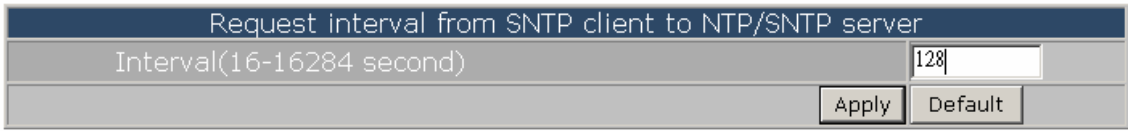
Example: Configure Server address as 10.1.1.1, configure version as 4, and then, Click Apply button to apply the configuration to switch.



15.4.2 Request interval configuration

Click “SNTP configuration”, “Request interval configuration” to configure the sending request time interval from SNTP client to NTP/SNTP server. Same as CLI command 15.1.2.

Example: Configure Interval as 128 minutes, Click Apply to set the configuration in the switch.

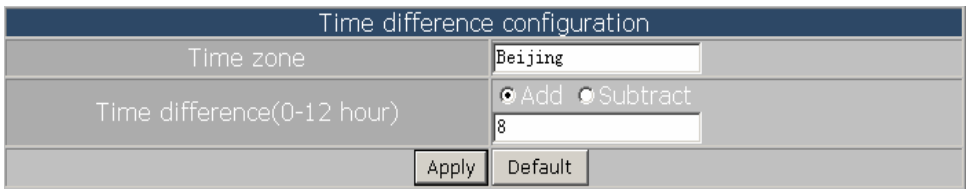


15.4.3 Time difference

Click “SNTP configuration”, “Time difference” to configure the SNTP client time zone and UTC time difference. Same as CLI command 15.1.3.

- Time zone – configures time zone
- Time difference – configures time difference
- Add – means the configured time zone is the + UTC time
- Subtract – means the configured time zone is the - UTC time

Example: Configure time zone as Beijing, select Add, set the time difference as 8, and then, click Apply to set the configuration in the switch .



15.4.4 Show SNMP

Click “SNTP configuration”, “Show sntp” to display the SNTP client current configuration and server status. Same as CLI command 15.3.1.1.

Chapter 16 QoS Configuration

16.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirements and network management policies.

16.1.1 QoS Terms

CoS: Class of Service, the classification information carried by Layer 2 IEEE 802.1Q frames. It takes 3 bits of the Tag field in the frame header for user priority level in the range of 0 to 7.

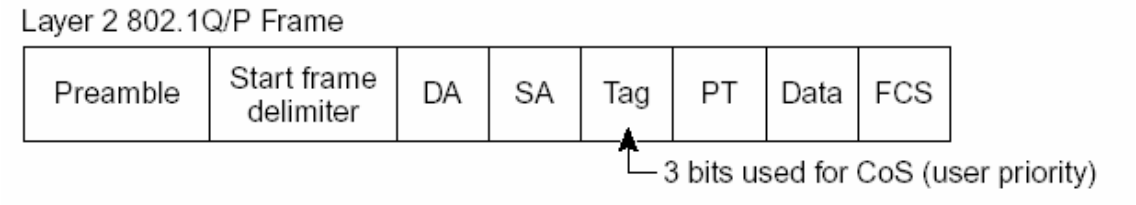


Fig 16-1 CoS priority

ToS: Type of Service, a one byte field carried in Layer 3 IPv4 packet headers to symbolize the service type of IP packets. The ToS field can be IP Precedence value or DSCP value.

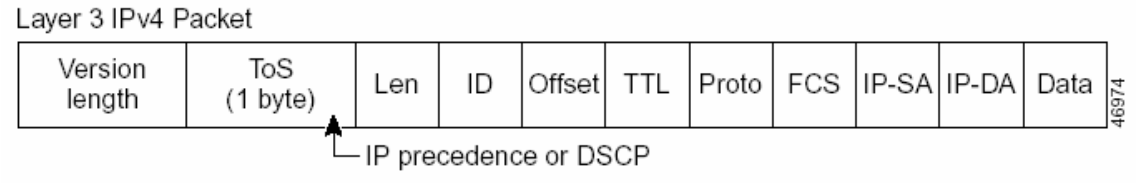


Fig 16-2 ToS priority

IP Precedence: IP priority, classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP: Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

Classification: The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing: Ingress action of QoS that lays down the policy and manages the classified packets.

Remark: Ingress action of QoS, performs allowing, degrading or discarding operations to packets according to the policies.

Queuing: Egress QoS action, put the packets to appropriate egress queues according to the packet CoS value.

Scheduling: QoS egress action, configure the weight for eight egress queue WRR (Weighted Round Robin).

In Profile: Traffic within the QoS policy range (bandwidth or burst value) is called “In Profile".

Out of Profile: Traffic out the QoS policy range (bandwidth or burst value) is called “Out of Profile".

16.1.2 QoS Implementation

To implement Layer 3 switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for current bandwidth resources. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or higher protocols such as TCP. However, rather providing and protecting packet transmission bandwidth, IP provides bandwidth service by best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-latency requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in the Layer 3 IP packet header or Layer 2 IEEE 802.1Q frame header. QoS provides same service to packets of the same priority, while offering different operations for packets of different priority. A QoS-enabled switch or router can provide different bandwidths according to the packet classification information, and can remark on the classification information according to the policing policies configured, and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology, devices and analysis to incoming/outgoing traffic.

16.1.3 Basic QoS Model

The basic QoS consists of five parts: Classification, Policing, Remarking, Queuing and Scheduling, Classification, policing and remarking are sequential ingress actions. Queuing and Scheduling are QoS egress actions.

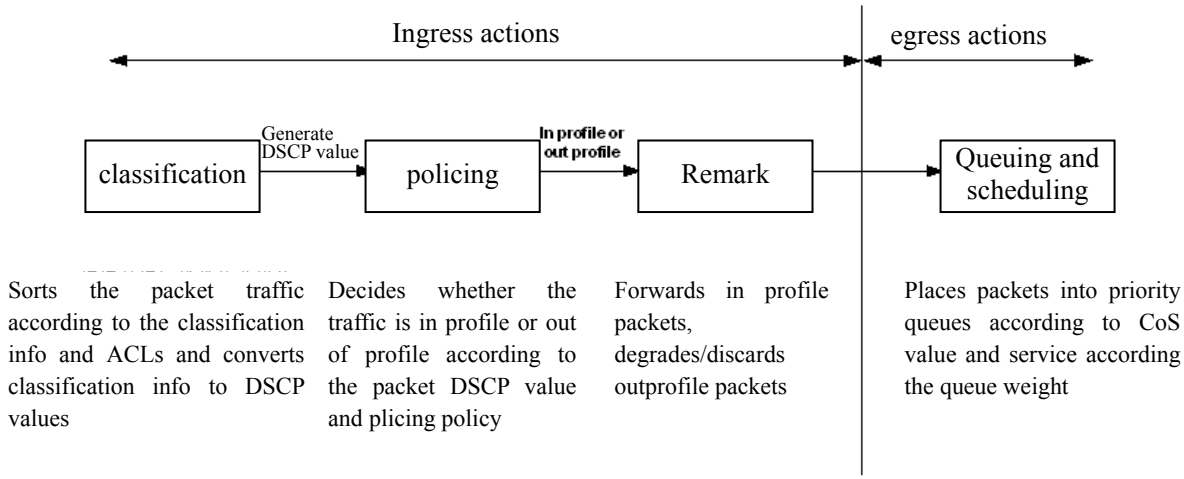

Ingress actions
egress actions
classification
Generate DSCP value
policing
In profile or out profile
Remark
Queuing and scheduling
Sorts the packet traffic according to the classification info and ACLs and converts classification info to DSCP values
Decides whether the traffic is in profile or out of profile according to the packet DSCP value and plicing policy
Forwards in profile packets, degrades/discards outprofile packets
Places packets into priority queues according to CoS value and service according the queue weight

Fig 16-3 Basic QoS Model

Classification: Classifies traffic according to packet classification information and generates internal DSCP value based on the classification information. For different packet types and switch configurations, classification is performed differently. The flowchart below explains this in detail.

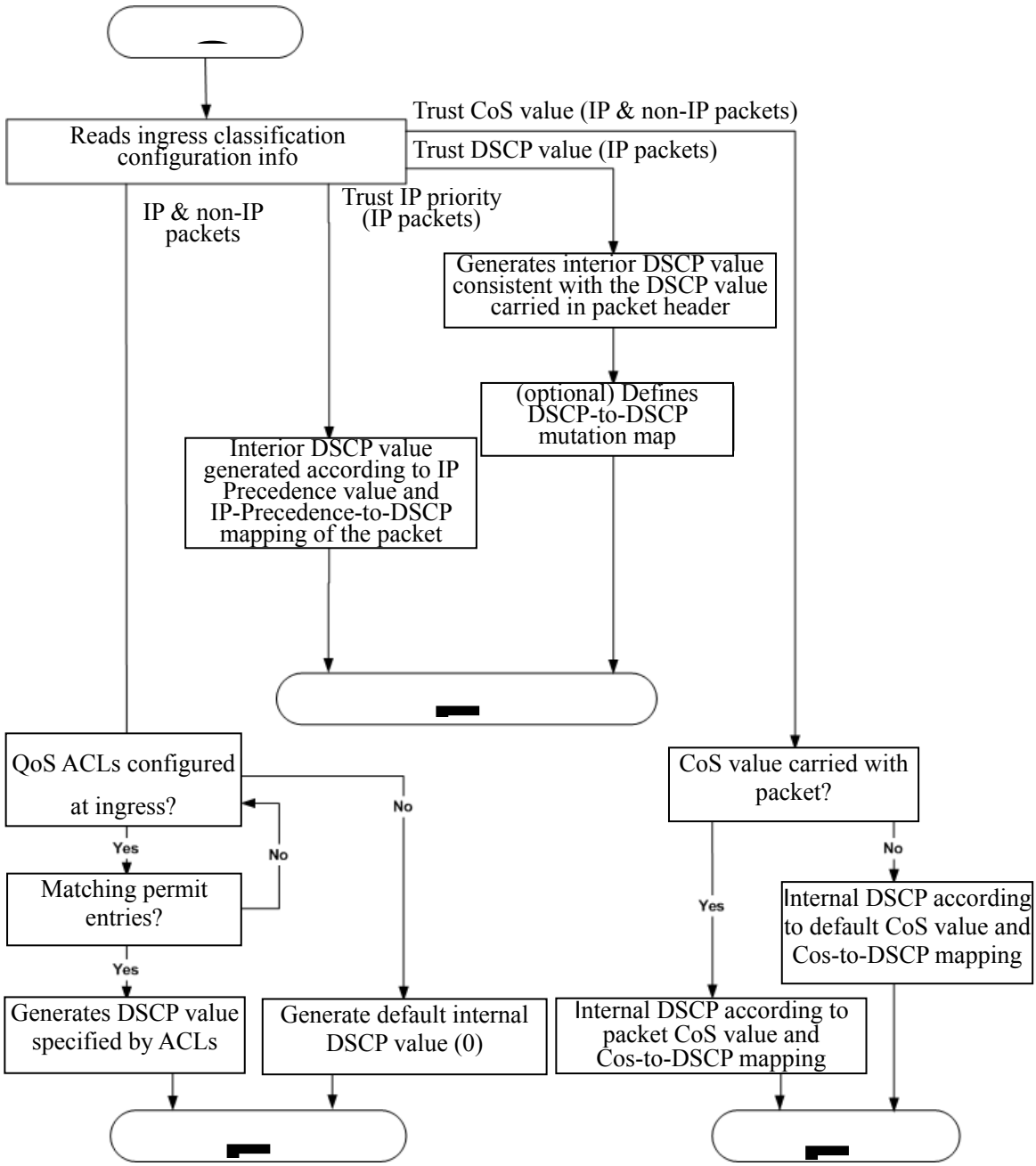

Reads ingress classification configuration info
Trust CoS value (IP & non-IP packets)
Trust DSCP value (IP packets)
Trust IP priority (IP packets)
IP & non-IP packets
Generates interior DSCP value consistent with the DSCP value carried in packet header
(optional) Defines DSCP-to-DSCP mutation map
Interior DSCP value generated according to IP Precedence value and IP-Precedence-to-DSCP mapping of the packet
QoS ACLs configured at ingress?
Yes
No
Matching permit entries?
Yes
No
Generates DSCP value specified by ACLs
Generate default internal DSCP value (0)
CoS value carried with packet?
Yes
No
Internal DSCP according to packet CoS value and Cos-to-DSCP mapping
Internal DSCP according to default CoS value and Cos-to-DSCP mapping

Fig 16-4 Classification process

Policing and remark: Each packet in classified ingress traffic is assigned an internal DSCP value and can be policed and remarked.

Policing can be performed based on DSCP value to configure different policies that allocate bandwidth to classified traffic. If the traffic exceeds the bandwidth set in the policy (out of profile), the out of profile traffic can be allowed, discarded or remarked. Remarking uses a new DSCP value of lower priority to replace the original higher level DSCP value in the packet; this is also called "marking down". The following flowchart describes the operations during policing and remarking.

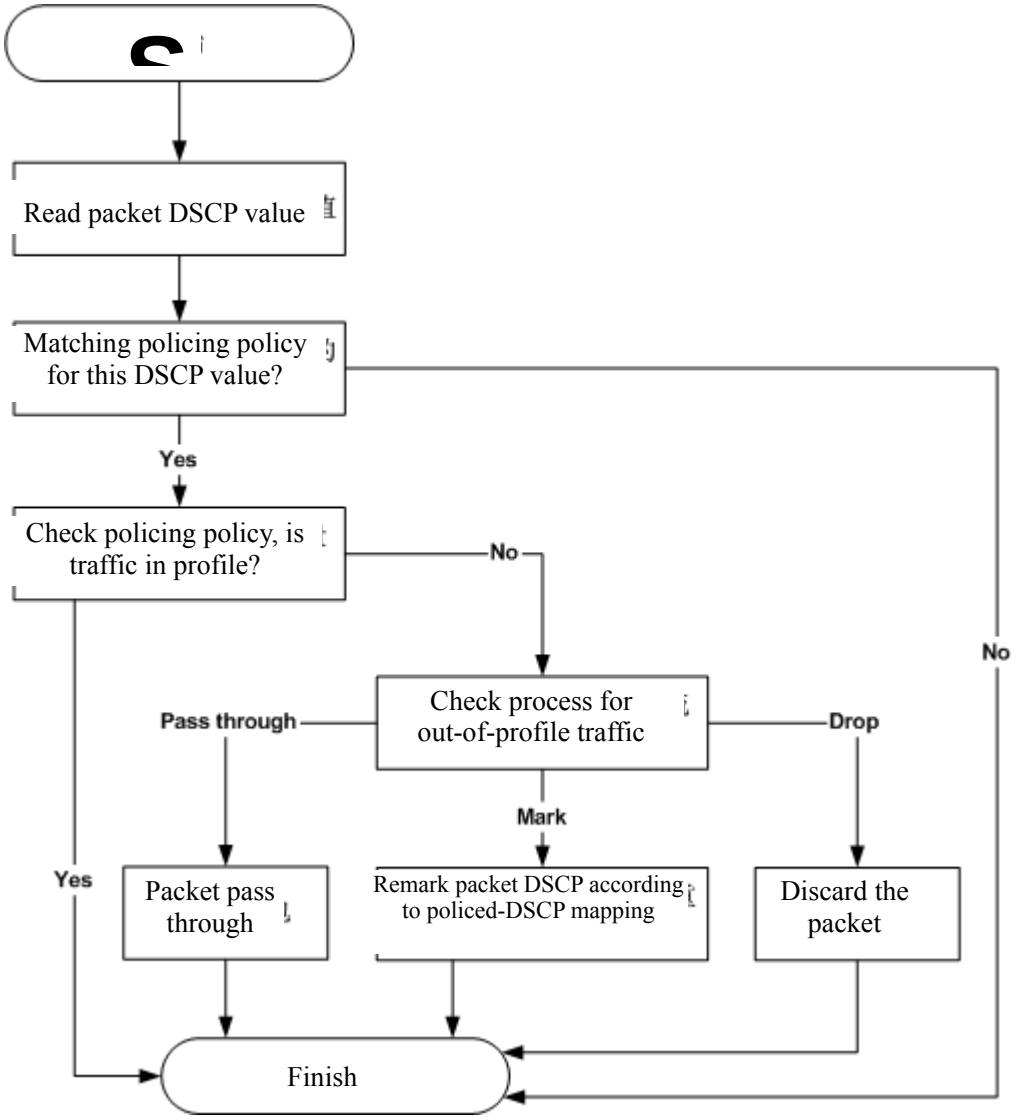


Fig 16-5 Policing and Remarking process

Queuing and scheduling: Packets at the egress will re-map the internal DSCP value to CoS value, the queuing operation assigns packets to appropriate queues of priority according to the CoS value; while the scheduling operation performs packet forwarding according to the prioritized queue weight. The following flowchart describes the operations during queuing and scheduling.

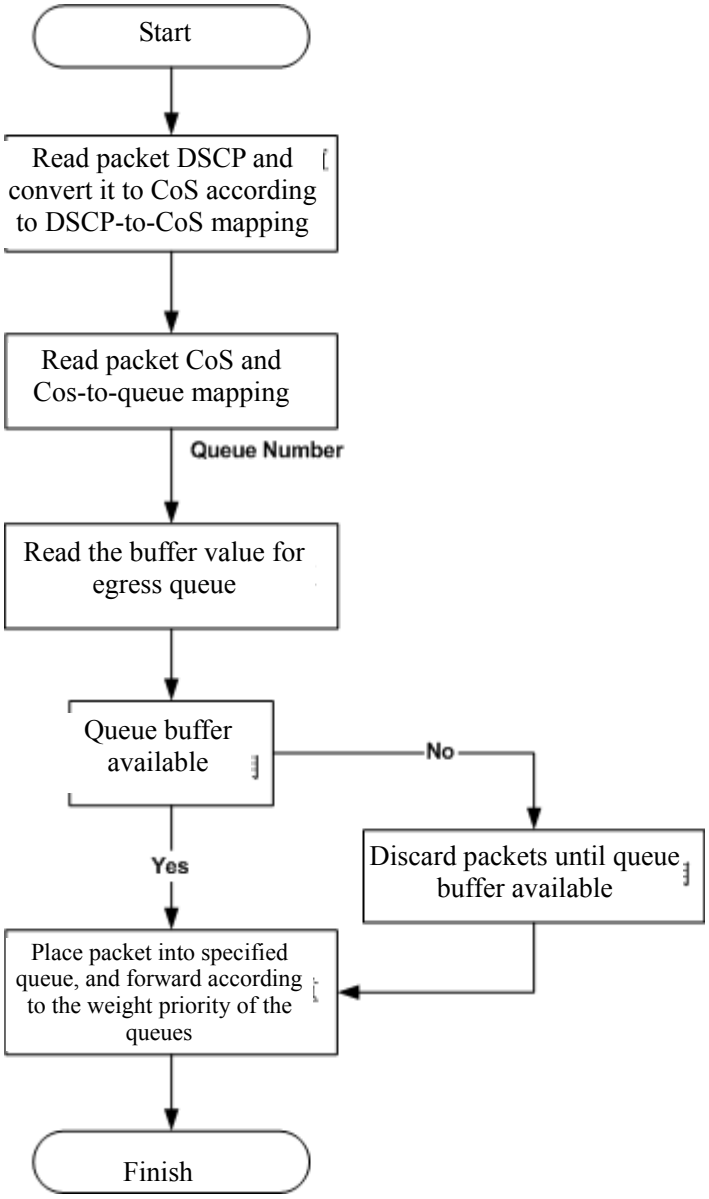

Start
Read packet DSCP and convert it to CoS according to DSCP-to-CoS mapping
Read packet CoS and Cos-to-queue mapping
Queue Number
Read the buffer value for egress queue
Queue buffer available
No
Yes
Discard packets until queue buffer available
Place packet into specified queue, and forward according to the weight priority of the queues
Finish

Fig 16-6 Queuing and Scheduling process

16.2 QoS Configuration

16.2.1 QoS Configuration Task Sequence

1. Enable QoS

   QoS can be enabled or disabled in Global Mode. QoS must be enabled first in Global Mode to configure other QoS commands.

2. Configure class map.

Set up a classification rule according to ACL, VLAN ID, IP Precedence or DSCP to classify the data stream. Different classes of data streams will be processed with different policies.

3. Configure a policy map.

After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading, assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be used in a policy map by several classes.

4. Apply QoS to the ports

Configures the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

5. Configure queue out method and weight

Configures queue out to PQ or WRR, sets the proportion of the 8 egress queues bandwidth and mapping from internal priority to egress queue.

6. Configure QoS mapping

Configures the mapping from CoS to DSCP, DSCP to CoS, DSCP to DSCP mutation, IP precedence to DSCP, and policed DSCP.

1. Enable QoS

Command	Explanation
Global Mode	
mls qos **no mls qos**	Enables/disables QoS function.

2. Configure class map

Command	Explanation
Global Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Creates a class map and enters class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.
match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| vlan <*vlan-list*>} **no match {access-group | ip dscp | ip precedence | vlan }**	Sets matching criterion (classify data stream by ACL, DSCP, VLAN or priority, etc) for the class map; the "**no match {access-group | ip dscp | ip precedence | vlan}**" command deletes specified matching criterion.

3. Configure a policy map

Command	Explanation
Global Mode	

policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Creates a policy map and enters policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.
class <*class-map-name*> **no class <*class-map-name*>**	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the "**no class <*class-map-name*>**" command deletes the specified class.
set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>} **no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**	Assigns a new DSCP and IP precedence value for the classified traffic; the "**no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**" command cancels the newly assigned value.
police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}] **no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**	Configures a policy to classify traffic, data stream exceeding the limit will be dropped or degraded; the "**no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.
mls qos aggregate-policer <*aggregate-policer-name*> <*rate-kbps*> <*burst-kbyte*> exceed-action {drop |policed-dscp-transmit} **no mls qos aggregate-policer <*aggregate-policer-name*>**	Defines a policy set, perform different actions to out-of-profile data streams, such as discard or degrade. This policy can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.
police aggregate <*aggregate-policer-name*> **no police aggregate <*aggregate-policer-name*>**	Applies a policy set to classified traffic; the "**no police aggregate <*aggregate-policer-name*>**" command deletes the specified policy set.

4. Apply QoS to ports

Command	Explanation
Interface Mode	
mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]|ip-precedence [pass-through cos]|port priority <*cos*>] **no mls qos trust**	Configures port trust; the "**no mls qos trust**" command disables the current trust status of the port.
mls qos cos {<*default-cos*> } **no mls qos cos**	Configures the default CoS value of the port; the "**no mls qos cos**" command restores the

	default setting.
service-policy {input <*policy-map-name*> | output <*policy-map-name*>} **no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**	Applies a policy map to the specified port; the "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" command deletes the specified policy map applied to the port. Egress policy map is not supported yet.
mls qos dscp-mutation <*dscp-mutation-name*> **no mls qos dscp-mutation <*dscp-mutation-name*>**	Applies DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

5. Configure queue out method and weight

Command	Explanation
Interface Mode	
wrr-queue bandwidth <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*> **no wrr-queue bandwidth**	Sets WRR weight for specified egress queue; the "**no wrr-queue bandwidth**" command restores the default setting.
priority-queue out **no priority-queue out**	Configures queue out method to pq method; the "**no priority-queue out**" command restores the default WRR queue out method.
Global Mode	
wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*> **no wrr-queue cos-map**	Sets CoS value mapping to specified egress queue; the "**no wrr-queue cos-map**" command restores the default setting.

6. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>} **no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**	Sets CoS to DSCP mapping, DSCP to CoS mapping, DSCP to DSCP mutation mapping, IP precedence to DSCP and policed DSCP mapping; the "**no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**" command restores the default mapping.

16.2.2 QoS Configuration Commands

16.2.2.1 mls qos

Command: mls qos

no mls qos

Function: Enables QoS in Global Mode; the "**no mls qos**" command disables the global QoS.

Command mode: Global Mode

Default: QoS is disabled by default.

Usage Guide: QoS provides 8 queues to handle traffics of 8 priorities. This function cannot be used with the traffic control function.

Example: Enabling and then disabling the QoS function.

Switch(Config)#mls qos

Switch(Config)#no mls qos

16.2.2.2 class-map

Command: class-map <*class-map-name*>

no class-map <*class-map-name*>

Function: Creates a class map and enters class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.

Parameters: <*class-map-name*> is the class map name.

Default: No class map is configured by default.

Command mode: Global Mode

Usage Guide:

Example: Creating and then deleting a class map named "c1".

Switch(Config)#class-map c1

Switch(Config-ClassMap)# exit

Switch(Config)#no class-map c1

16.2.2.3 match

Command: match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| vlan <*vlan-list*>}

no match {access-group | ip dscp | ip precedence | vlan }

Function: Configures the matching criterion in the class map; the "**no match {access-group | ip dscp | ip precedence | vlan}**" command deletes the specified matching criterion.

Parameters: access-group <*acl-index-or-name*> stands for matching specified ACL, the parameter is ACL number or name; **ip dscp <*dscp-list*>** stands for matching specified DSCP value, the parameter is a DSCP value list containing up to 8 DSCP values; **ip precedence <*ip-precedence-list*>** stands for matching specified IP priority, the parameter is a IP priority list containing up to 8 IP priorities, ranging from 0 to 7; **vlan <*vlan-list*>** stands for matching specified VLAN ID list

consisting of up to 8 VLAN Ids.

Default: No matching criterion is configured by default.

Command mode: Class map configuration mode

Usage Guide: Only one matching criterion is allowed in each class map. When matching ACLs, only "permit" rule can be set in the ACL.

Example: Creating a class map named c1, setting the class map rule to match packets of IP precedence priority 0 and 1.

Switch(Config)#class-map c1

Switch(Config-ClassMap)#match ip precedence 0 1

Switch(Config-ClassMap)#exit

16.2.2.4 policy-map

Command: policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

Function: Creates a policy map and enters the policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.

Parameters: < *policy-map-name*> is the policy map name.

Default: No policy map is configured by default.

Command mode: Global Mode

Usage Guide: QoS classification matching and marking operations can be done in the policy map configuration mode.

Example: Creating and deleting a policy map named "p1".

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#exit

Switch(Config)#no policy-map p1

16.2.2.5 class

Command: class <*class-map-name*>

no class <*class-map-name*>

Function: Associates a class to a policy map and enters the policy class map mode; the "**no class <*class-map-name*>**" command deletes the specified class.

Parameters: < *class-map-name*> is the class map name used by the class.

Default: No policy class is configured by default.

Command mode: Policy map configuration Mode

Usage Guide: Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy map mode, classification and policy configuration can be performed on packet traffic classified by class map.

Example: Entering a policy class mode.

Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#exit

16.2.2.6 set

Command: set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}
no set {ip dscp | ip precedence}

Function: Assigns a new DSCP and IP precedence value for the classified traffic; the "**no set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>}**" command cancels the newly assigned value.

Parameters: **<*new-dscp*>** is the new DSCP value; **<*new-precedence*>** is the new IP precedence value.

Default: No value is assigned by default.

Command mode: Policy class map configuration Mode

Usage Guide: Only traffic satisfying the matching criterion and those classified will be assigned new values.

Example: Setting the IP Precedence value of packets satisfying c1 class rule to 3.

Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#set ip precedence 3
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit

16.2.2.7 police

Command: police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]
no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]

Function: Configures a policy to a classified traffic; the "**no police <*rate-kbps*> <*burst-kbyte*> [exceed-action {drop | policed-dscp-transmit}]**" command deletes the specified policy.

Parameters: **<*rate-kbps*>** is the average baud rate (kb/s) of classified traffic, ranging from 1,000 to 10,000,000; **exceed-action drop** means drop packets when specified speed is exceeded; **exceed-action policed-dscp-transmit** specifies to mark down packet DSCP value according to **policed-dscp** mapping when specified speed is exceeded.

Default: There is no policy by default.

Command mode: Policy class map configuration Mode

Usage Guide: The ranges of **<*rate-kbps*>** and **<*burst-kbyte*>** are quite large, if the setting exceeds the actual speed of the port, the policy map applying this policy will not bind to switch ports.

Example: Setting the bandwidth for packets that matching c1 class rule to 20 Mbps, with a burst

value of 2 MB, all packets exceed this bandwidth setting will be dropped.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config--Policy-Class)#police 20000 2000 exceed-action drop

Switch(Config--Policy-Class)#exit

Switch(Config-PolicyMap)#exit

16.2.2.8 mls qos aggregate-policer

Command: mls qos aggregate-policer <*aggregate-policer-name*> <*rate-kbps*> <*burst-kbyte*> exceed-action {drop |policed-dscp-transmit}

no mls qos aggregate-policer <*aggregate-policer-name*>

Function: Defines a policy set that can be used in one policy map by several classes; the "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command deletes the specified policy set.

Parameters: **<*aggregate-policer-name*>** is the name of the policy set; **<*rate-kbps*>** is the average baud rate (in kb/s) of classified traffic, range from 1,000 to 10,000,000; **<*burst-kbyte*>** is the burst value (in kb/s) for classified traffic, range from 1 to 1,000,000; **exceed-action drop** means drop packets when specified speed is exceeded; **exceed-action policed-dscp-transmit** specifies to mark down packet DSCP value according to **policed-dscp** mapping when specified speed is exceeded.

Default: No policy set is configured by default.

Command mode: Global Mode

Usage Guide: If a policy set is using by a policy map, it cannot be deleted unless the reference to the policy set is cleared in the appropriate policy map with "**no police aggregate <*aggregate-policer-name*>**" command. The delete should be performed in Global Mode with "**no mls qos aggregate-policer <*aggregate-policer-name*>**" command.

Example: Setting a policy set named "agg1", the policy set defines the bandwidth for packets of up to 20 Mbps, with a burst value of 2 MB. All packets exceeding this bandwidth setting will be dropped.

Switch(Config)#mls qos aggregate-policer agg1 20000 2000 exceed-action drop

16.2.2.9 police aggregate

Command: police aggregate <*aggregate-policer-name*>

no police aggregate <*aggregate-policer-name*>

Function: Applies a policy set to classified traffic; the "**no police aggregate <*aggregate-policer-name*>**" command deletes the specified policy set.

Parameters: **<*aggregate-policer-name*>** is the policy set name.

Default: No policy set is configured by default.

Command mode: Policy class map configuration Mode

Usage Guide: The same policy set can be referred to by different policy class maps.

Example: Appling a policy set "agg1" to packets satisfying c1 class rule.

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config--Policy-Class)#police aggregate agg1

Switch(Config--Policy-Class)#exit

Switch(Config-PolicyMap)#exit

16.2.2.10 mls qos trust

Command: mls qos trust [cos [pass-through-dscp]|dscp [pass-through-cos]| ip-precedence [pass-through-cos] |port priority <*cos*>]

[no] mls qos trust

Function: Configures port trust; the "**no mls qos trust**" command disables the current trust status of the port.

Parameters: cos configures the port to trust CoS value; **cos pass-through-dscp** configures the port to trust CoS value but does not change packet DSCP value; **dscp** configures the port to trust DSCP value; **dscp pass-through-cos** configures the port to trust DSCP value, but does not change packet CoS value; **ip-precedence** configures the port to trust IP precedence; **ip-precedence pass-through-cos** configures the port to trust IP precedence, but does not change packet CoS value.

port priority <***cos***> assigns a priority to the physical port, **cos** is the priority to be assigned. Priority of all incoming packets through the port will be set to this cos value. This is irrelevant to the priority of the packet itself, no modification is done to the packets.

Default: No trust.

Command mode: Interface Mode

Usage Guide: For packets with both CoS value and DSCP value, keyword **pass-through** should be used to protect the value if the value should not be changed after classification.

Example: Configuring Ethernet port 1/1 to trust CoS value, i.e., classifying the packets according to CoS value, DSCP value should not be changed.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos trust cos pass-through-dscp

16.2.2.11 mls qos cos

Command: mls qos cos {<*default-cos*> }

no mls qos cos

Function: Configures the default CoS value of the port; the "**no mls qos cos**" command restores the

default setting.

Parameters: < ***default-cos***> is the default CoS value for the port, the valid range is 0 to 7.

Default: The default CoS value is 0.

Command mode: Interface Mode

Usage Guide:

Example: Setting the default CoS value of Ethernet port 1/1 to 5, i.e., packets coming in through this port will be assigned a default CoS value of 5 if no CoS value present.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos cos 5

16.2.2.12 service-policy

Command: service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

Function: Applies a policy map to the specified port; the "**no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}**" command deletes the specified policy map applied to the port.

Parameters: input <*policy-map-name*> applies the specified policy map to the ingress of switch port; **output <*policy-map-name*>** applies the specified policy map to the egress of switch port.

Default: No policy map is bound to ports by default.

Command mode: Interface Mode

Usage Guide: Configuring port trust status and applying policy map on the port are two conflicting operations; the later configuration will override the earlier configuration. Only one policy map can be applied to each direction of each port. Egress policy map is not supported yet.

Example: Binding policy p1 to ingress of Ethernet port 1/1.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)# service-policy input p1

16.2.2.13 mls qos dscp-mutation

Command: mls qos dscp-mutation <*dscp-mutation-name*>

no mls qos dscp-mutation <*dscp-mutation-name*>

Function: Applies DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

Parameters: <*dscp-mutation-name*> is the DSCP mutation mapping name.

Default: There is no policy by default.

Command mode: Interface Mode

Usage Guide: For configuration of DSCP mutation mapping on the port to take effect, the trust

status of that port must be “trust DSCP”. Applying DSCP mutation mapping allows DSCP values specified directly to be converted into new DSCP values without class and policy process. DSCP mutation mapping is effective to the local port only. “trust DSCP” refers to the DSCP value before DSCP mutation in this case.

Example: Configuring Ethernet port 1/1 to trust DSCP, using DSCP mutation mapping of mu1.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos trust dscp pass-through cos

Switch(Config-Ethernet1/1)#mls qos dscp-mutation mu1

16.2.2.14 wrr-queue bandwidth

Command: wrr-queue bandwidth <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*>

no wrr-queue bandwidth

Function: Sets the WRR weight for specified egress queue; the “**no wrr-queue bandwidth**” command restores the default setting.

Parameters: <*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*> are WRR weights, ranging from 0 to 15.

Default: The default values of weight1 to weight8 are 1 through 8. .

Command mode: Interface Mode

Usage Guide: The absolute value of WRR is meaningless. WRR allocates bandwidth by using eight weight values. If a weight is 0, then the queue has the highest priority; when the weights of multiple queues are set to 0, then the queue of higher order has the higher priority.

Example: Setting the bandwidth weight proportion of the eight queue out to be 1:1:2:2:4:4:8:8.

Switch(Config-Ethernet1/1)#wrr-queue bandwidth 1 1 2 2 4 4 8 8

16.2.2.15 priority-queue out

Command: priority-queue out

no priority-queue out

Function: Configures the queue out mode. The “**no priority-queue out**” command restores the default value and default queue out weights.

Parameters:

Default: non-priority-queue mode.

Command mode: Interface Mode

Usage Guide: When priority-queue out mode is used, packets are no longer sent with WRR algorithm, but sent by packets queue after queue.

Example: Setting the queue out mode to priority-queue.

Switch(Config-Ethernet1/1)#priority-queue out

16.2.2.16 wrr-queue cos-map

Command: wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>

no wrr-queue cos-map

Function: Sets the CoS value mapping to the specified queue out; the "**no wrr-queue cos-map**" command restores the default setting.

Parameters: **<*queue-id*>** is the ID of queue out, ranging from 1 to 8; **<*cos1 ... cos8*>** are CoS values mapping to the queue out, ranging from 0 – 7, up to 8 values are supported.

Default:

Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	0	1	2	3	4	5	6	7
Queue Selected	1	2	3	4	5	6	7	8

Command mode: Global Mode

Usage Guide:

Example: Mapping packets with CoS value 2 and 3 to egress queue 1.

Switch(Config)#wrr-queue cos-map 1 2 3

16.2.2.17 mls qos map

Command: mls qos map {cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp <*dscp-list*> to <*mark-down-dscp*>}

no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}

Function: Sets **class of service (CoS)-to-Differentiated Services Code Point (DSCP)** mapping, **DSCP to CoS** mapping, **DSCP to DSCP mutation** mapping, **IP precedence to DSCP** and **policed DSCP** mapping; the "**no mls qos map {cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp}**" command restores the default mapping.

Parameters: **cos-dscp <*dscp1...dscp8*>** defines the mapping from CoS value to DSCP, **<*dscp1...dscp8*>** are the 8 DSCP value corresponding to the 0 to 7 CoS value, each DSCP value is delimited with space, ranging from 0 to 63; **dscp-cos <*dscp-list*> to <*cos*>** defines the mapping from DSCP to CoS value, **<*dscp-list*>** is a list of DSCP value consisting of up to 8 DSCP values, **<*cos*>** are the CoS values corresponding to the DSCP values in the list; **dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*>** defines the mapping from DSCP to DSCP mutation, **<*dscp-mutation-name*>** is the name for mutation mapping, **<*in-dscp*>** stand for incoming DSCP values, up to 8 values are supported, each DSCP value is delimited with space, ranging from 0 to 63, **<*out-dscp*>** is the sole outgoing DSCP value, the 8 values defined in incoming DSCP will be converted to outgoing DSCP values;

ip-prec-dscp <*dscp1...dscp8*> defines the conversion from IP precedence to DSCP value, **<*dscp1...dscp8*>** are 8 DSCP values corresponding to IP precedence 0 to 7, each DSCP value is delimited with space, ranging from 0 to 63; **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** defines DSCP **mark down** mapping, where **<*dscp-list*>** is a list of DSCP values containing up to 8 DSCP values, **<*mark-down-dscp*>** are DSCP value after **mark down**.

Default: Default mapping values are:

Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-CoS Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS Value	0	1	2	3	4	5	6	7

Default IP-Precedence-to-DSCP Map

IP Precedence Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

dscp-mutation and policed-dscp are not configured by default

Command mode: Global Mode

Usage Guide: In **police** command, classified packet traffic can be set to mark down if exceed specified average speed or burst value, **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** can mark down the DSCP values of those packets to new DSCP values.

Example: Setting the ***CoS-to-DSCP*** mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7.

Switch(Config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7

16.3 QoS Example

Scenario 1:

Enable QoS function, change the queue out weight of Ethernet port 1/1 to 1:1:2:2:4:4:8:8, and set the port in trust CoS mode without changing DSCP value, and set the default CoS value of the port to 5.

The configuration steps are listed below:

SWITCH#CONFIG

Switch(Config)#mls qos
Switch(Config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#wrr-queue bandwidth 1 1 2 2 4 4 8 8
Switch(Config-Ethernet1/1)#mls qos trust cos pass-through dscp
Switch(Config-Ethernet1/1)#mls qos cos 5

Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of Ethernet port 1/1 is 1:1:2:2:4:4:8:8. When packets have CoS value coming in through Ethernet port 1/1 , they will be map to the queue according to this value. CoS values range from 0 to 7 and correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8, respectively. If the incoming packet has no CoS value, it is by default 5 and will be put in queue 6. All passing packets would not have their DSCP values changed.

Scenario 2:

In Ethernet port 1/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mbps, with a burst value of 4 MB and all packets exceeding this bandwidth setting will be dropped.

The configuration steps are listed below:

SWITCH#CONFIG

Switch(Config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(Config)#mls qos
Switch(Config)#class-map c1
Switch(Config-ClassMap)#match access-group 1
Switch(Config-ClassMap)# exit
Switch(Config)#policy-map p1
Switch(Config-PolicyMap)#class c1
Switch(Config--Policy-Class)#police 10000 4000 exceed-action drop
Switch(Config--Policy-Class)#exit
Switch(Config-PolicyMap)#exit
Switch(Config)#interface ethernet 1/2
Switch(Config-Ethernet1/2)#service-policy input p1

Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. QoS was enabled globally, a class map named c1 was created, matching ACL1 in class map; another policy map named p1 was created and refers to c1 in p1, appropriate policies were set to limit bandwidth and burst value. This policy map was applied on Ethernet port 1/2. After the above settings were done, bandwidth for packets from segment 192.168.1.0 through Ethernet port 1/2 is was set to 10 Mbps, with a burst value of 4 MB, all packets exceeding this bandwidth setting in that segment will be dropped.

Scenario 3:

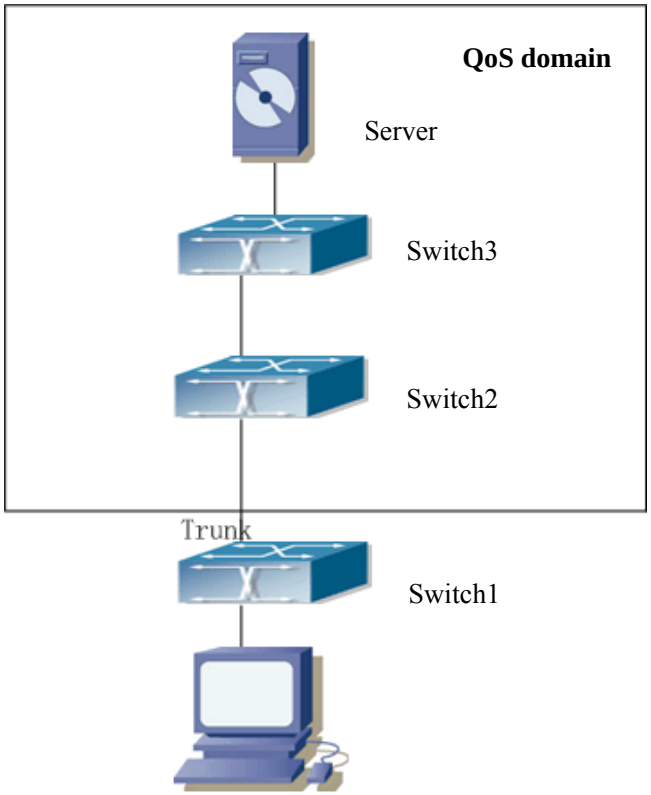


Fig 16-7 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, switch1 classifies different traffic and assigns different IP precedence. For example, set IP precedence for packets from segment 192.168.1.0 to 5 on Ethernet port 1/1. The port connecting to switch2 is a trunk port. In Switch2, set Ethernet port 1/1 that connecting to swtich1 to trust IP precedence. Thus inside the QoS domain, packets of different priority will go to different queues and get different bandwidth.

The configuration steps are listed below:

QOS CONFIGURATION IN SWITCH1:

SWITCH#CONFIG

Switch(Config)#access-list 1 permit 192.168.1.0 0.0.0.255

Switch(Config)#mls qos

Switch(Config)#class-map c1

Switch(Config-ClassMap)#match access-group 1

Switch(Config-ClassMap)# exit

Switch(Config)#policy-map p1

Switch(Config-PolicyMap)#class c1

Switch(Config--Policy-Class)#set ip precedence 5

Switch(Config--Policy-Class)#exit

Switch(Config-PolicyMap)#exit

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#service-policy input p1

QoS configuration in Switch2:

SWITCH#CONFIG

Switch(Config)#mls qos

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#mls qos trust ip-precedence pass-through-cos

16.4 QoS Troubleshooting Help

16.4.1 QoS Debug and Monitor Commands

16.4.1.1 show mls-qos

Command: show mls-qos

Function: Displays global configuration information for QoS.

Parameters: N/A.

Default: N/A.

Command mode: Admin Mode

Usage Guide: This command indicates whether QoS is enabled or not.

Example:

Switch #show mls-qos

Qos is enabled

Displayed information	Explanation
Qos is enabled	QoS is enabled.

16.4.1.2 show mls qos aggregate-policer

Command: show mls qos aggregate-policer [<*aggregate-policer-name*>]

Function: Displays policy set configuration information for QoS.

Parameters: **<*aggregate-policer-name*>** is the policy set name.

Default: N/A.

Command mode: Admin Mode

Usage Guide:

Example:

Switch #show mls qos aggregate-policer policer1

aggregate-policer policer1 80000 80 exceed-action drop

Not used by any policy map

Displayed information	Explanation
aggregate-policer policer1 80000 80 exceed-action drop	Configuration for this policy set.
Not used by any policy map	Time that the policy set is being referred to

16.4.1.3 show mls qos interface

Command: show mls qos interface [<*interface-id*>] [buffers | policers | queueing | statistics]

Function: Displays QoS configuration information on a port.

Parameters: <***interface-id***> is the port ID; **buffers** is the queue buffer setting on the port; **policers** is the policy setting on the port; **queuing** is the queue setting for the port; **statistics** is the number of packets allowed to pass for in-profile and out-of-profile traffic according to the policy bound to the port.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Statistics are available only when ingress policy is configured.

Example:

Switch #show mls qos interface ethernet 1/2

Ethernet1/2

default cos:0

DSCP Mutation Map: Default DSCP Mutation Map

Attached policy-map for Ingress: p1

Displayed information	Explanation
Ethernet1/2	Port name
default cos:0	Default CoS value of the port.
DSCP Mutation Map: Default DSCP Mutation Map	Port DSCP map name
Attached policy-map for Ingress: p1	Policy name bound to port.

Switch # show mls qos interface buffers ethernet 1/2

Ethernet1/2

packet number of 8 queue:

0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200

Displayed information	Explanation
packet number of 8 queue: 0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200	Available packet number for all 8 queues out on the port, this is a fixed setting that cannot be changed.

Switch # show mls qos interface queueing ethernet 1/2

Switch#show mls qos int queue e 1/2

Cos-queue map:

Cos 0 1 2 3 4 5 6 7

Queue 1 2 3 4 5 6 7 8

Queue and weight type:

Port q1 q2 q3 q4 q5 q6 q7 q8 QType

Ethernet1/2 1 2 3 4 5 6 7 8 WFQ

Displayed information	Explanation
Cos-queue map:	CoS value to queue mapping.
Queue and weight type:	Queue to weight mapping.
QType	WFQ or PQ queue out method

Switch # show mls qos interface policers ethernet 1/2

Ethernet1/2

Attached policy-map for Ingress: p1

Displayed information	Explanation
Ethernet1/2	Port name
Attached policy-map for Ingress: p1	Policy map bound to the port.

Switch # show mls qos interface statistics ethernet 1/2

Device: Ethernet1/2

Classmap classified in-profile out-profile (in packets)

c1 0 0 0

Displayed information	Explanation
Ethernet1/2	Port name
ClassMap	Name of the Class map
classified	Total data packets match this class map.
in-profile	Total in-profile data packets match this class map.
out-profile	Total out-profile data packets match this class map.

16.4.1.4 show mls qos maps

Command: show mls qos maps [cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp]

Function: Displays mapping configuration information for QoS.

Parameters: cos-dscp CoS for CoS-DSCP; **dscp-cos** DSCP for DSCP-CoS, **dscp-mutation <*dscp-mutation-name*>** for DSCP-DSCP mutation, **<*dscp-mutation-name*>** is the name

of mutation; **ip-prec-dscp** IP for IP precedence-DSCP; **policed-dscp** is DSCP mark down mapping.

Default: N/A.

Command mode: Admin Mode

Usage Guide:

Example:

Switch # show mls qos map

Cos-dscp map:

cos:	0	1	2	3	4	5	6	7
dscp:	0	8	16	24	32	40	48	56

IpPrecedence-dscp map:

ipprec:	0	1	2	3	4	5	6	7
dscp:	0	8	16	24	32	40	48	56

Dscp-cos map:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0:	0	0	0	0	0	0	0	0	1	1
1:	1	1	1	1	1	1	2	2	2	2
2:	2	2	2	2	3	3	3	3	3	3
3:	3	3	4	4	4	4	4	4	4	4
4:	5	5	5	5	5	5	5	5	6	6
5:	6	6	6	6	6	6	7	7	7	7
6:	7	7	7	7						

Policed-dscp map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

0: 0 1 2 3 4 5 6 7 8 9

1: 10 11 12 13 14 15 16 17 18 19

2: 20 21 22 23 24 25 26 27 28 29

3: 30 31 32 33 34 35 36 37 38 39

4: 40 41 42 43 44 45 46 47 48 49

5: 50 51 52 53 54 55 56 57 58 59

6: 60 61 62 63

16.4.1.5 show class-map

Command: show class-map [<*class-map-name*>]

Function: Displays class map of QoS.

Parameters: < *class-map-name*> is the class map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Displays all configured class-map or specified class-map information.

Example:

Switch # show class-map

Class map name:c1

Match acl name:1

Displayed information	Explanation
Class map name:c1	Name of the Class map
Match acl name:1	Classifying rule for the class map.

16.4.1.6 show policy-map

Command: show policy-map [<*policy-map-name*>]

Function: Displays policy map of QoS.

Parameters: < *policy-map-name*> is the policy map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Displays all configured policy-map or specified policy-map information.

Example:

Switch # show policy -map

Policy Map p1
  Class Map name: c1
    police 16000000 2000 exceed-action drop

Displayed information	Explanation
Policy Map p1	Name of policy map
Class map name:c1	Name of the class map referred to
police 16000000 8000 exceed-action drop	Policy implemented

16.4.2 QoS Troubleshooting Help

- QoS is disabled on switch ports by default, 8 sending queues are set by default, queue1 forwards normal packets, other queues are used for some important control packets (such as BPDU).
- When QoS is enabled in Global Mode,. QoS is enabled on all ports with 8 traffic queues. The default CoS value of the port is 0; port is in not Trusted state by default; the default queue weight values are 1, 2, 3, 4, 5, 6, 7, 8 in order, all QoS Map uses the default value.
- CoS value 7 maps to queue 8 that has the highest priority and usually reserved for certain protocol packets. It is not recommended for the user to change the mapping between CoS 7 to Queue 8, or set the default port CoS value to 7.
- Policy map can only be bound to ingress direction, egress is not supported yet.
  If the policy is too complex to be configured due to hardware resource limits, error massages will be provided.

16.5 WEB MANAGEMENT

Select “QoS configuration”. It consists of the following sections:

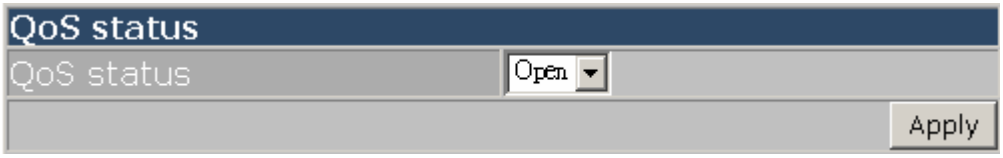
- Enable QoS
- Class-map configuration
- Policy-map configuration
- Apply QoS to port

16.5.1 Enable QoS

Click “Enable QoS” to display the extension, select Enable/Disable QoS then enter the configure page. Equivalent to CLI command 16.2.2.1.

- QoS status－Close or Open.

To enable QoS, select Open, then click Apply.



16.5.2 Class-map configuration

Click “Class-map configuration” to display the extension, including the following two sections:

1. Add/Remove class-map
2. Class-map configuration

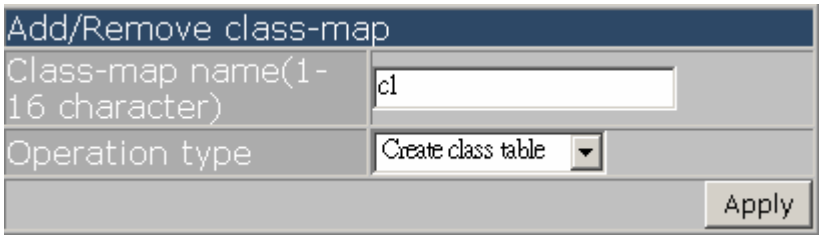
16.5.2.1 Add/Remove class-Map

Click “Add/Remove class-map” to enter configuration page. Equivalent to CLI command 16.2.2.2.

Term description as follows:

- Class-map name
- Operation type－Create class table and Remove class table.

Example: Enter a class-map name, select Create class table, then click Apply.



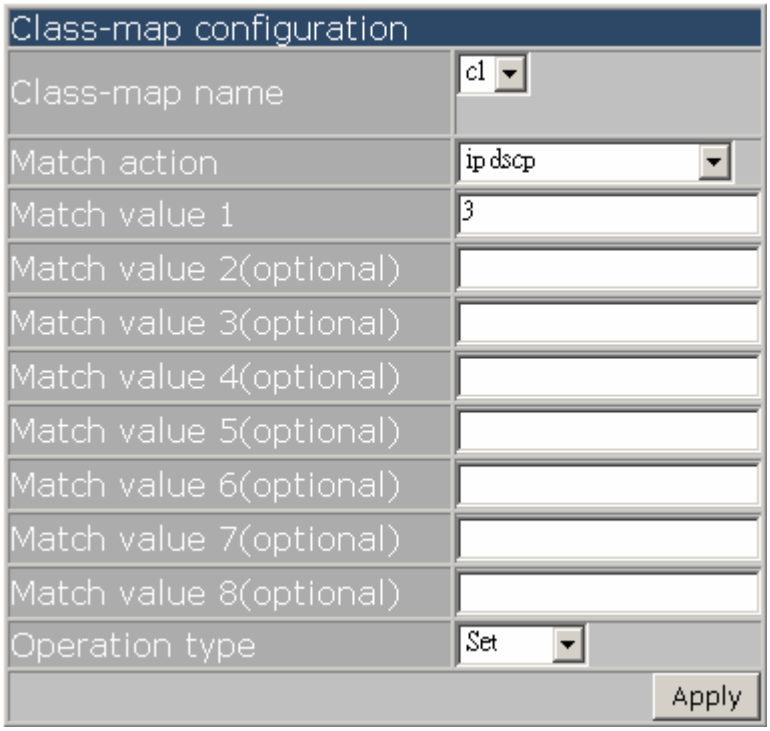
16.5.2.2 Class-map configuration

Click “Class-map configuration” to enter the configuration page. Equivalent to CLI command 16.2.2.3.

Terms are described as following:

- Class-map name
- Match action which including:
  - ✓ **access-group First valid**－mapping to ACL table. Parameter is the assign number or name of ACL. First valid means Match value 1 is valid.
  - ✓ **ip dscp**－mapping to DSCP. Parameter is the DSCP value list.
  - ✓ **ip precedence**－mapping to IP priority. Parameter is IP priority value list.
  - ✓ **vlan**－mapping to VLAN ID. Parameter is VLAN ID value list.
  - ✓ **Match value 1-8**－mapping to parameter value table. Input ACL value to match value 1 for mapping ACL.
  - ✓ **Operation type**－Sets or Removes.

To configure Class-map c1, select c1 to Class-map name, select ip dscp to Match action, input 3 to Match value 1, select set to Operation type, and then click Apply.



16.5.3 Policy-map priority configuration

Click “Policy-map configuration” to display the extension, which has five sections:

- Add/Remove policy-map
- Policy-map priority configuration
- Policy-map bandwidth configuration
- Add/Remove aggregate policer
- Apply aggregate policer

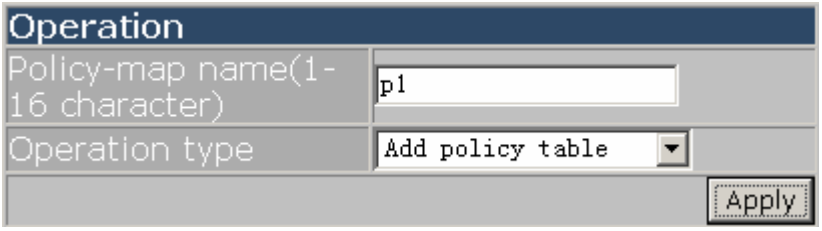
16.5.3.1 Add/Remove policy-map

Click “Add/Remove policy-map” to enter the configuration page. Equivalent to CLI command 16.2.2.4.

Terms are described as following:

- Policy-map name
- Operation type. Add policy table or Remove policy table.

Example: Set policy-map name as p1, select Add policy table, then click Apply to add policy table.



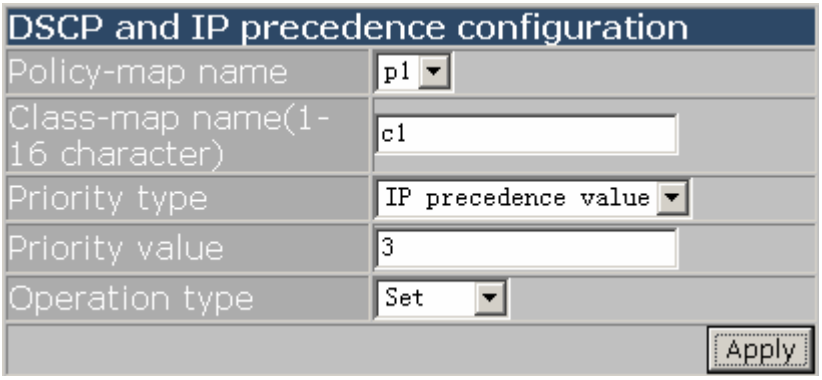
16.5.3.2 Policy-map priority configuration

Click "Policy-map priority configuration" to entry configure page. Equivalent to CLI command 16.2.2.6.

Terms are described as following:

- Policy-map name
- Class-map name
- Priority type. DSCP value or IP precedence value
- Priority value
- Operation type. Set or Remove.

Example: Select p1 to Policy-map name, input c1 to Class-map name, select IP precedence value to Priority type, input 3 to Priority value, select Set to Operation type, and then click Apply.



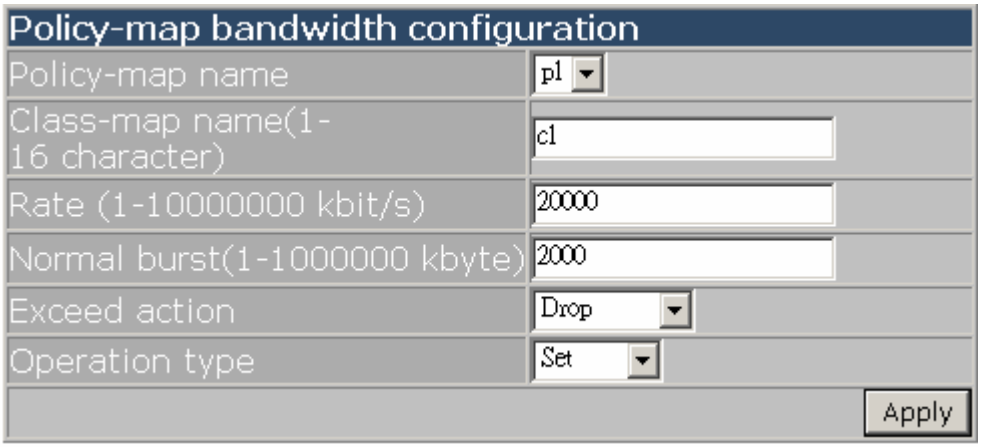
16.5.3.3 Policy-map bandwidth configuration

Click "Policy-map bandwidth configuration" to entry configure page. Equivalent to CLI command 16.2.2.7.

Terms are described as following:

- Policy-map name
- Class-map name
- Rate—average baud rate for classified bandwidth, K bit/s per unit.
- Normal burst—burst rate for classified bandwidth, K byte per unit.
- Exceed action—The action for once the data rate exceeds the rate limited, includes drop and policied-dscp-transmit, the latter is by a mapping function between given DSCP and corresponding policy and mark the DSCP into the packet.
- Operation type—Set or Remove.

To configure Policy-map bandwidth configuration, select p1 to Policy-map name, input c1 to Class-map name, all sections choose as default setting, select Set to Operation type, and then click Apply.



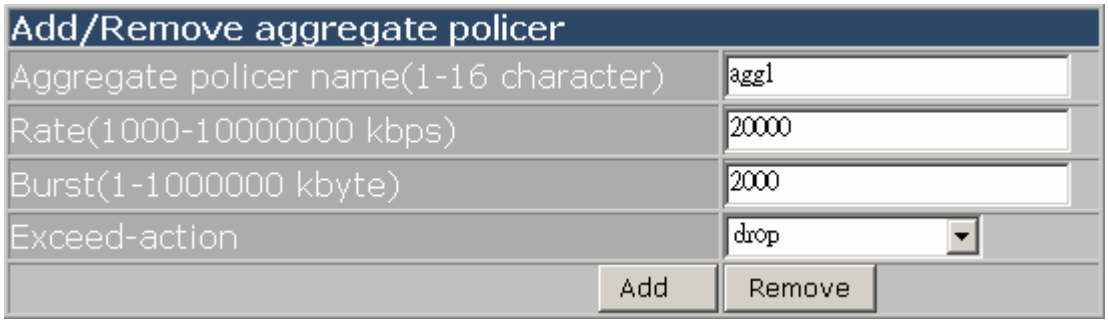
16.5.3.4 Add/Remove aggregate policy

Click Add/Remove aggregate policer to entry configure page. It is equivalent to CLI command 16.2.2.8.

Terms are described as following:

- Aggregate policer name
- Rate—average baud rate for classified bandwidth, K bit/s per unit.
- Burst—burst rate for classified bandwidth, K byte per unit.
- Exceed-action—The action for once the data rate exceeds the rate limited, includes drop and policied-dscp-transmit, the latter is by a mapping function between given DSCP and corresponding policy and mark the DSCP into the packet.

To create the aggregate-policer, named as agg1, the definition of aggregate-policer is based on the baud rate 20M Kbps, the burst rate 2M Kbyte. All packets will be dropped whenever over the assigned running rate. After setting all value, then click Add.



16.5.3.5 Apply aggregate policy

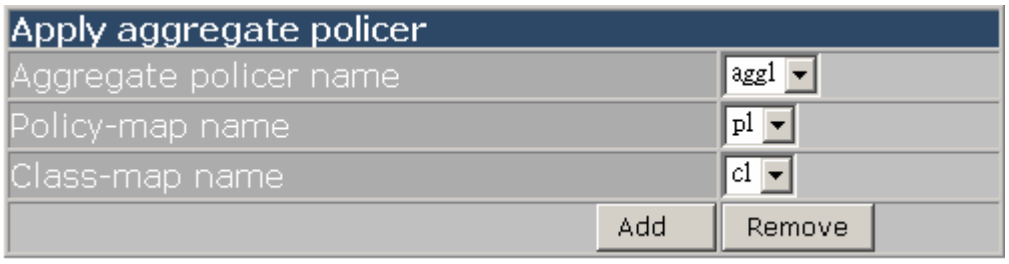
Click "Apply aggregate policer" to enter the configuration page. Equivalent to CLI command 16.2.2.9.

Terms are described as following:

- Aggregate policer name
- Policy-map name
- Class-map name

Example: Apply the aggregate policer agg1 by c1 class-map, input the graphic presentation value,

and then click Add.



16.5.4 Apply QoS to port

Click "Apply QoS to port" to enter the configuration page, which include four sections:

- Port trust mode configuration
- Port default CoS configuration
- Apply policy-map to port
- Apply DSCP mutation mapping

16.5.4.1 Port trust mode configuration

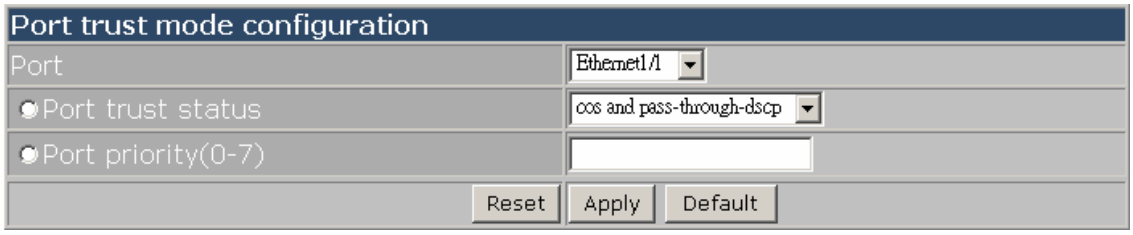
Click "Port trust mode configuration" to enter the configuration page. Equivalent to CLI command 16.2.2.10.

Terms are described as following:

- Port
- Port trust status－including
  - ✓ cos, cos and pass-through-dcsp,
  - ✓ dcsp, dcsp and pass-through-cos,
  - ✓ ip-precedence, ip-pre and pass-through-cos
- Port priority
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Apply－Will take effort to all setting. This command will modify the configuration.
- Default－Will back to startup setting. This command will modify the configuration.

The parameter will take effect alternative port trust status and port priority.

Example: Configuring the Ethernet port 1/1 with trust mode, setting packet as COS value classification first and keep it without changing DSCP value. Choosing the Ethernet1/1 port and select the cos and pass-through-dcsp for Port trust status, then click Apply.



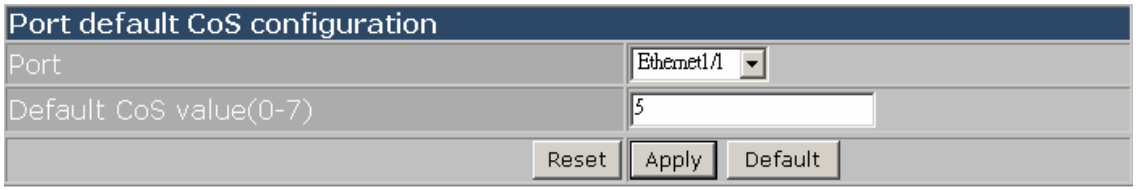
16.5.4.2 Port default CoS configuration

Click "Port default CoS configuration" to entry configure page. Equivalent to CLI command 16.2.2.11.

Terms are described as following:

- Port
- Default CoS value—Startup CoS value
- Reset—Will set column as startup defaults. This command will not modify the configuration.
- Apply—Will take effort to all setting. This command will modify the configuration.
- Default—Will back to startup setting. This command will modify the configuration.

Example: Setting the CoS value as 5 in Ethernet port 1/1 and click Apply to finish.



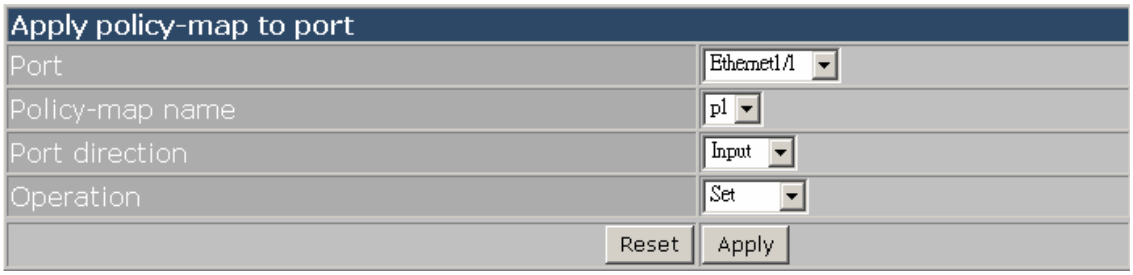
16.5.4.3 Apply policy-map to port

Click "Apply policy-map to port" to enter the configuration page. Equivalent to CLI command 16.2.2.12.

Terms are described as following:

- Port
- Policy-map name
- Port direction—Input or Output
- Operation—Set or Remove
- Reset—Will set column as startup defaults. This command will not modify the configuration.
- Apply—Will take effort to all setting. This command will modify the configuration.

Example: Choose Ethernet1/1 for port and p1 for policy-map; select Input for port direction and Set for operation, then click Apply.



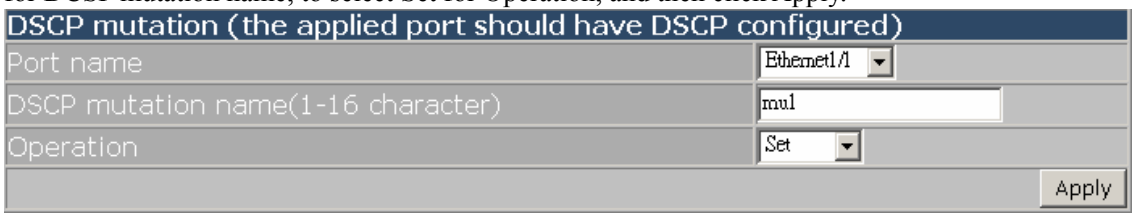
16.5.4.4 Apply DSCP mutation mapping

Click "Apply DSCP mutation mapping" to enter the configuration page. Equivalent to CLI command 16.2.2.13.

Terms are described as following:

- Port name
- DSCP mutation name
- Operation—Set or Remove

Example: Set the DSCP mutation in Ethernet port 1/1. Choose Port name as Ethernet1/1, input mu1 for DCSP mutation name, to select Set for Operation, and then click Apply.



16.5.5 Egress-queue configuration

Click "Egress-queue configuration" to display the extensions, including three sections:

1. Egress-queue wrr weight configuration
2. Egress-queue work mode configuration
3. Mapping CoS values to egress queues

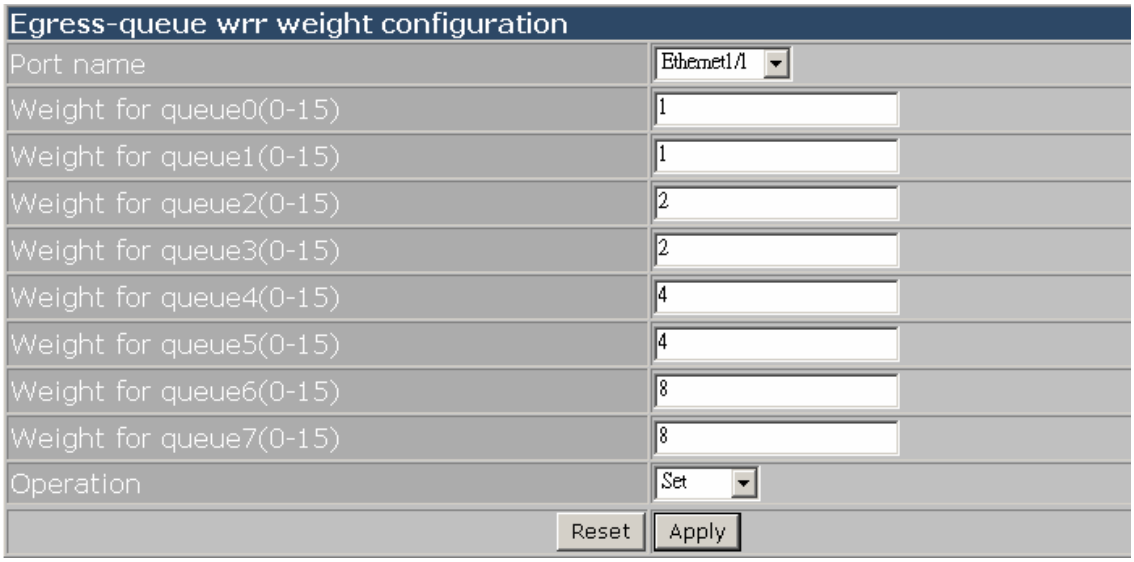
16.5.5.1 Egress-queue WRR weight configuration

Click "Egress-queue WRR weight configuration" to enter the configuration page. Equivalent to CLI command 16.2.2.14.

Terms are described as following:

- Port name
- Weight for queue 0-7
- Operation－Set or Remove
- Reset－Will set column as startup defaults. This command will not modify the configuration.
- Apply－Will take effort to all setting. This command will modify the configuration.

Example: Configuring WRR weight. Choose the port name first, then input value for each queue; select Set for operation, then click Apply.



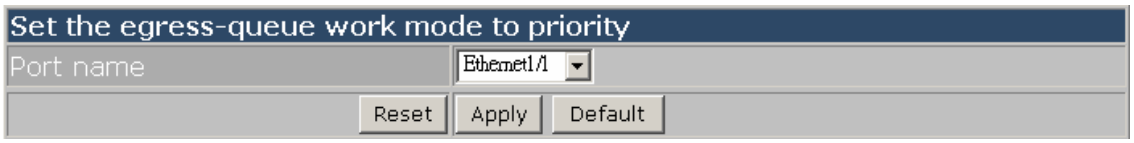
16.5.5.2 Egress-queue Work mode configuration

Click "Egress-queue work mode configuration" to enter the configuration page. Equivalent to CLI command 16.2.2.15.

Terms are described as following:

- Port name
- Reset—Will set column as startup defaults. This command will not modify the configuration.
- Apply—Will take effort to all setting. This command will modify the configuration.
- Default—Will back to startup setting. This command will modify the configuration.

Example: Configure the port as priority-queue mode: chose port name first, and then click Apply.



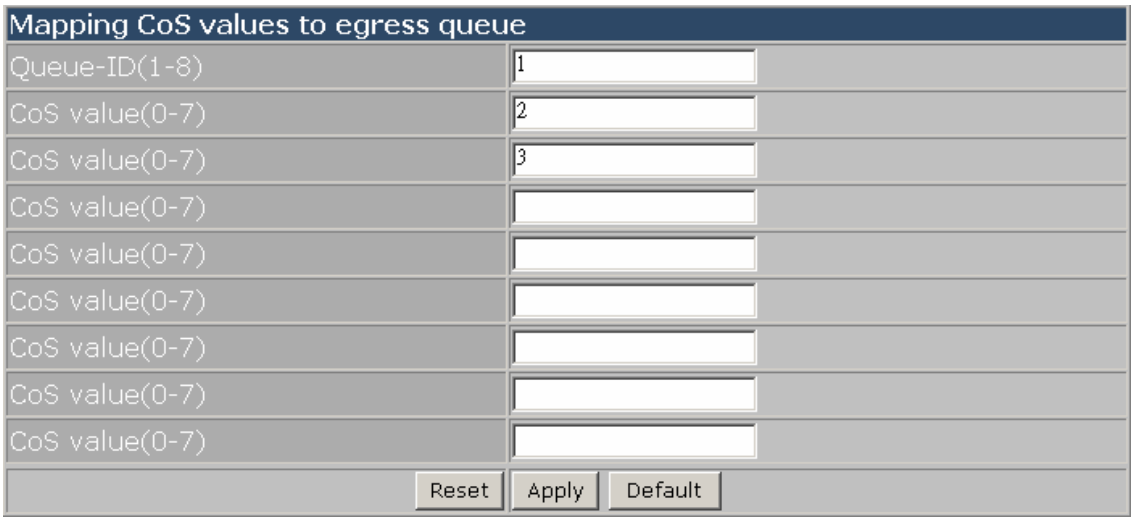
16.5.5.3 Mapping CoS values to egress queue

Click "Mapping CoS values to egress queue" to enter the configuration page. Equivalent to CLI command 16.2.2.16.

Terms are described as following:

- Queue-ID
- CoS value—Mapping CoS values to Egress queue. Up to 8 queue to be supported.
- Reset—Will set column as startup defaults. This command will not modify the configuration.
- Default—Will reset to startup settings. This command will modify the configuration.

Example: set the packet with CoS value 2/3 to mapping egress queue 1, the Queue-ID should be set as 1 and CoS value set with value 2/3, then click Apply.



16.5.6 QoS mapping configuration

Click "QoS mapping configuration" to display extensions, including the following:

1. CoS-to-DSCP mapping
2. DSCP-to-CoS mapping
3. DSCP mutation mapping

4. IP-Precedence-to-DSCP mapping
5. DSCP mark down mapping

These configurations are equivalent to CLI command16.2.2.17

16.5.6.1 CoS-to-DSCP mapping

Click “CoS-to-DSCP mapping” to enter the configuration page.

Terms are described as following:

- CoS－CoS value 0-7
- DSCP－Up to 8 DSCP mutations and mapping to CoS value 0～7
- Operation－Set or Remove

Example: To apply CoS value 2 to map DSCP value 20, input the DSCP value 20 in CoS value 2 column, selecting Set for Operation type, then click Apply.

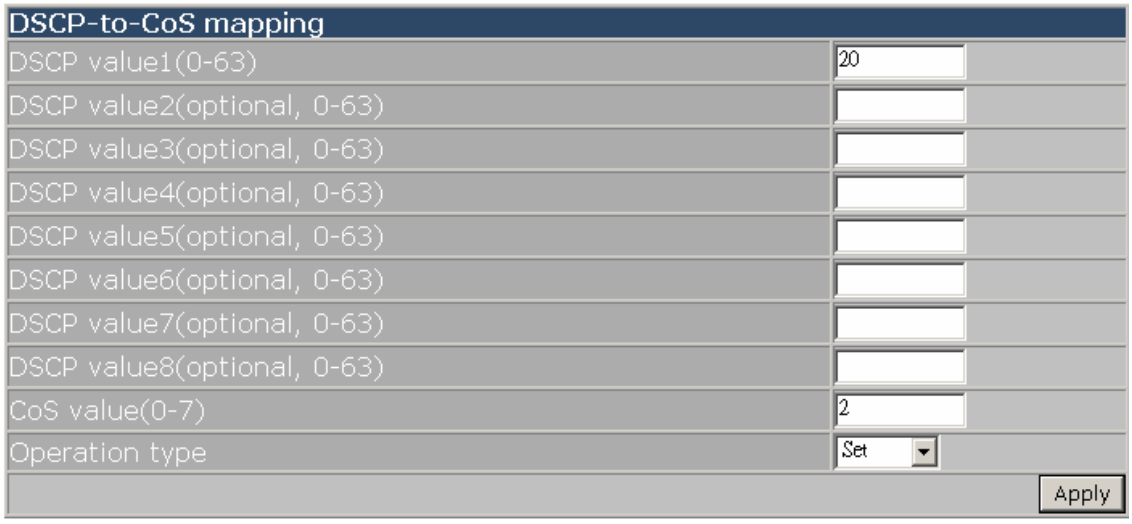
16.5.6.2 DSCP-to-CoS mapping

Click “DSCP-to-CoS mapping” to entry configure page.

Terms are described as following:

- DSCP 1-8－DSCP value
- CoS Value－DSCP value mapping to CoS value
- Operation type－Add or Remove

Example: To make DSCP value 20 map to CoS value 2, input the CoS value 2 and DSCP1 value 20, selecting Set for Operation type, then click Apply.

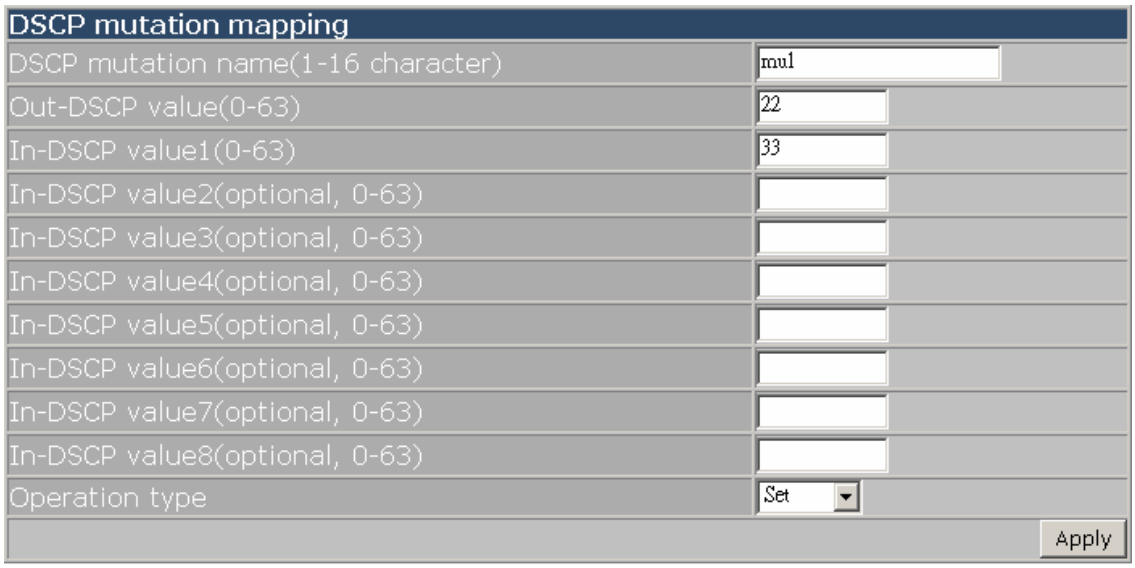


16.5.6.3 DSCP mutation mapping

Click “DSCP mutation mapping” to enter the configuration page.

Terms are described as following:

- DSCP mutation name
- Out-DSCP value
- In-DSCP value1-8
- Operation type－Set or Remove



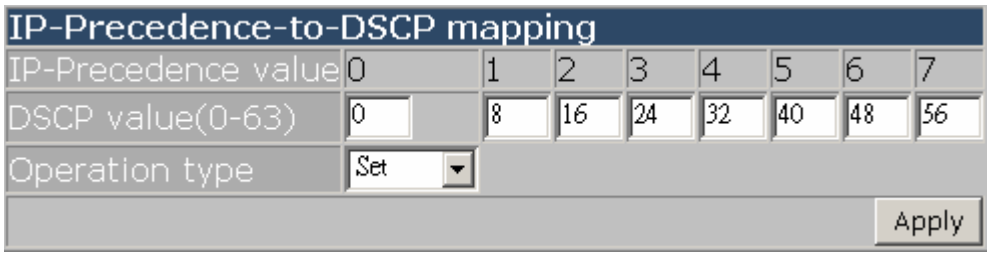
16.5.6.4 IP-precedence-to-DSCP mapping

Click “IP-Precedence-to-DSCP mapping” to enter the configuration page.

Terms are described as following:

- IP-Precedence－IP precedence value 0～7
- DSCP－IP precedence value mapping to DSCP value
- Operation type－Sets or Removes

Example: to set the IP precedence value 2 to map to DSCP value 20, input the DSCP value 20 into the IP precedence value 2 column, selecting Set for Operation type, then click Apply.



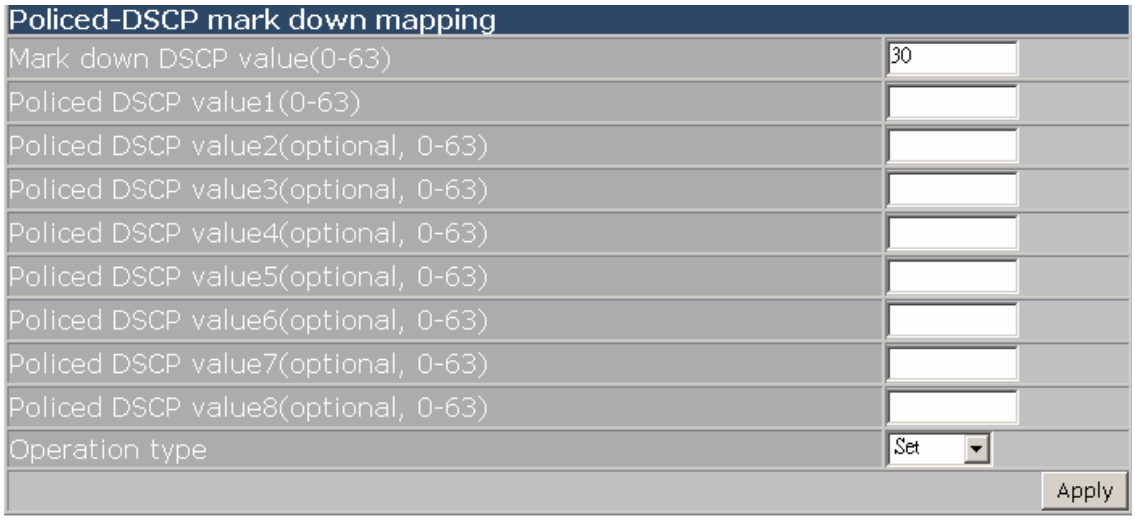
16.5.6.5 DSCP mark down mapping

Click “DSCP mark down mapping” to enter the configuration page.

Terms are described as following:

- Mark down dscp value
- Policed DSCP value1-8－DSCP value table
- Operation type－Set or Remove

Example: To set the DSCP value 10/20 to mark down to 30, set Mark down DSCP value as 30 first and policed DSCP 1/2 for value10/20, selecting Set for Operation type, then click Apply.



Chapter 17 L3 Forward Configuration

ES4704BD supports Layer 3 forwarding which forwards Layer 3 protocol packets (IP packets) across VLANs. Such forwarding uses IP addresses, when a port receives a IP packet, it will index it in its own route table and decide the operation according to the index result. If the IP packet is destined to another subnet reachable from this switch, then the packet will be forwarded from the appropriate port. ES4704BD can forward IP packets by hardware, the forwarding chip of ES4704BD has a host route table and default route table. Host route table stores host routes to connect to the switch directly; default route table stores segment routes (after aggregation algorithm process).

If the route (either host route or segment route) for forwarding unicast traffic exists in the forwarding chip, rather than processing by the CPU in router, the forwarding of traffic will be completely handled by hardware. As a result, forwarding speed can be greatly improved, even to line speed.

17.1 Layer 3 Interface

17.1.1 Introduction to Layer 3 Interface

Layer 3 interface can be created on ES4704BD. Layer 3 interface is not physical interface but a virtual interface. Layer 3 interface is built on VLANs. The Layer 3 interface can contain one or more layer2 interfaces of the same VLAN, or no layer2 interfaces. At least one of the Layer2 interfaces contained in Layer 3 interface should be in a UP state for Layer 3 interface in the UP state, otherwise, Layer 3 interface will be in the DOWN state. All layer 3 interfaces in the switch use the same MAC address, this address is selected from the reserved MAC address in creating Layer 3 interface. The Layer 3 interface is the base for layer 3 protocols. The switch can use the IP addresses set in the layer 3 interface to communicate with the other devices via IP. The switch can forward IP packets between different Layer 3 interfaces.

17.1.2 Layer 3 interface configuration

17.1.2.1 Layer 3 Interface Configuration Task Sequence

1. Create Layer 3 Interface

Command	Explanation
Global Mode	
interface vlan <*vlan-id*>	Creates a VLAN interface (VLAN interface is a

no interface vlan <*vlan-id*>	Layer 3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the VLAN interface (Layer 3 interface) created in the switch.

17.1.2.2 Layer 3 Interface Configuration Commands

17.1.2.2.1 interface vlan

Command: interface vlan <*vlan-id*>

no interface vlan <*vlan-id*>

Function: Creates a VLAN interface (a Layer 3 interface); the "**no interface vlan <*vlan-id*>**" command deletes the Layer 3 interface specified.

Parameters: <*vlan-id*> is the VLAN ID of the established VLAN.

Default: No Layer 3 interface is configured upon switch shipment.

Command mode: Global Mode

Usage Guide: When crating a VLAN interface (Layer 3 interface), VLANs should be configured first, for details, see the VLAN chapters. When VLAN interface (Layer 3 interface) is created with this command, the VLAN interface (Layer 3 interface) configuration mode will be entered. After the creation of the VLAN interface (Layer 3 interface), interface vlan command can still be used to enter Layer 3 interface mode.

Example: Creating a VLAN interface (layer 3 interface).

Switch (Config)#interface vlan 1

17.2 IP Forwarding

17.2.1 Introduction to IP Forwarding

Gateway devices can forward IP packets from one subnet to another; such forwarding uses routes to find a path. IP forwarding of ES4704BD is done with the participation of hardware and so wire speed forwarding can be achieved. In addition, flexible management is provided to adjust and monitor forwarding. ES4704BD supports aggregation algorithm enabling/disabling optimization to adjust segment route generation in the switch chip and view statistics for IP forwarding and hardware forwarding chip status.

17.2.2 IP Route Aggregation Configuration

17.2.2.1 IP Route Aggregation Configuration Task

1. Set whether IP route aggregation algorithm with/without optimization should be used.

Command	Explanation
ip fib optimize **no ip fib optimize**	Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

17.2.2.2 IP Route Aggregation Configuration Command

17.2.2.2.1 ip fib optimize

Command: ip fib optimize

no ip fib optimize

Function: Enables the switch to use optimized IP route aggregation algorithm; the "**no ip fib optimize**" disables the optimized IP route aggregation algorithm.

Default: Optimized IP route aggregation algorithm is disabled by default.

Command mode: Global Mode

Usage Guide: This command is used to optimize the aggregation algorithm: if the route table contains no default route, the next hop most frequently referred to will be used to construct a virtual default route to simplify the aggregation result. This method has the benefit of more effectively simplifying the aggregation result. However, while adding a virtual default route to the chip segment route table reduces CPU load, it may introduce unnecessary data stream to switches of the next hop. In fact, part of local switch CPU load is transferred to switches of the next hop.

Example: Disabling optimized IP route aggregation algorithm.

Switch(Config)# no ip fib optimize

17.2.3 IP Forwarding Troubleshooting Help

17.2.3.1 Monitor and Debug Commands

17.2.3.1.1 show ip traffic

Command: show ip traffic

Function: Display statistics for IP packets.

Command mode: Admin Mode

Usage Guide: Display statistics for IP and ICMP packets received/sent.

Example:

Switch#show ip traffic

IP statistics:

Rcvd: 128 total, 128 local destination

```
        0 header errors, 0 address errors
        0 unknown protocol, 0 discards
  Frags: 0 reassembled, 0 timeouts
        0 fragment rcvd, 0 fragment dropped
        0 fragmented, 0 couldn't fragment, 0 fragment sent
  Sent:  0 generated, 0 forwarded
        0 dropped, 0 no route
ICMP statistics:
  Rcvd:  0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
  Sent:  0 total 0 errors 0 time exceeded
        0 redirects, 0 unreachable, 0 echo, 0 echo replies
        0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 timestamp replies
TCP statistics:
  TcpActiveOpens          0, TcpAttemptFails      0
  TcpCurrEstab            0, TcpEstabResets       0
  TcpInErrs               0, TcpInSegs            0
  TcpMaxConn              0, TcpOutRsts           0
  TcpOutSegs              0, TcpPassiveOpens      0
  TcpRetransSegs          0, TcpRtoAlgorithm      0
  TcpRtoMax               0, TcpRtoMin            0
UDP statics:
  UdpInDatagrams          0, UdpInErrors          0
  UdpNoPorts              0, UdpOutDatagrams      0
```

Displayed information	Explanation
IP statistics：	IP packet statistics.
Rcvd： 290 total, 44 local destinations 0 header errors, 0 address errors 0 unknown protocol, 0 discards	Statistics of total packets received, number of packets reached local destination, number of packets have header errors, number of erroneous addresses, number of packets of unknown protocols; number of packets dropped.
Frags： 0 reassembled, 0 timeouts 0 fragment rcvd, 0 fragment dropped 0 fragmented, 0 couldn't fragment, 0 fragment sent	Fragmentation statistics: number of packets reassembled, timeouts, fragments received, fragments discarded, packets that cannot be

	fragmented, number of fragments sent, etc.
Sent： 0 generated, 0 forwarded 0 dropped, 0 no route	Statistics for total packets sent, including number of local packets, forwarded packets, dropped packets and packets without route.
ICMP statistics：	ICMP packet statistics.
Rcvd： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets received and classified information
Sent： 0 total 0 errors 0 time exceeded 0 redirects, 0 unreachable, 0 echo, 0 echo replies 0 mask requests, 0 mask replies, 0 quench 0 parameter, 0 timestamp, 0 timestamp replies	Statistics of total ICMP packets sent and classified information
TCP statistics:	TCP packet statistics.
UDP statistics:	UDP packet statistics.

17.2.3.1.2 debug ip packet

Command: debug ip packet
no debug ip packet
Function: Enable the IP packet debug function: the "no debug IP packet" command disables this debug function.
Default: IP packet debugging information is disabled by default.
Command mode: Admin Mode
Usage Guide: Displays statistics for IP packets received/sent, including source/destination address and bytes, etc.
Example: Enabling IP packet debug.
Switch#debug ip pa
ip packet debug is on
Switch#
Switch#
Switch#
Switch#%Apr 19 15:56:33 2005 IP PACKET: rcvd, src 192.168.2.100, dst 192.168.2.1
, size 60, Ethernet0

17.3 ARP

17.3.1 Introduction to ARP

ARP (Address Resolution Protocol) is mainly used in IP address to Ethernet MAC address resolution. ES4704BD supports both dynamic ARP and static configuration. Furthermore, ES4704BD supports the configuration of proxy ARP for some applications. For instance, when an ARP request is received on the port, requesting an IP address in the same IP segment of the port but not the same physical network, if the port has enabled proxy ARP, the port would reply to the ARP with its own MAC address and forward the actual packets received. Enabling proxy ARP allows machines physically separated but of the same IP segment ignores the physical separation and communicate via proxy ARP interface as if in the same physical network.

17.3.2 ARP configuration

17.3.2.1 ARP Configuration Task Sequence

1. Configure static ARP
2. Configure proxy ARP

1. Configure static ARP

Command	Explanation
arp <*ip_address*> <*mac_address*> {[ethernet] <*portName*>} **no arp <*ip_address*>**	Configures a static ARP entry; the "**no arp <*ip_address*>"** command deletes a static ARP entry.

2. Configure proxy ARP

Command	Explanation
ip proxy-arp **no ip proxy-arp**	Enables the proxy ARP function for Ethernet ports: the "**no ip proxy-arp"** command disables the proxy ARP.

17.3.2.2 ARP Forwarding Configuration Commands

17.3.2.2.1 Arp

Command: arp <*ip_address*> <*mac_address*> {[ethernet] <*portName*>}

no arp <*ip_address*>

Function: Configures a static ARP entry; the "**no arp <*ip_address*>"** command deletes a static ARP entry.

Parameters: <*ip_address*> is the IP address; **<*mac_address*>** is the MAC address; **ethernet** stands for Ethernet port; **<*portName*>** for the name of layer2 port.

Default: No static ARP entry is set by default.

Command mode: VLAN Interface Mode

Usage Guide: Static ARP entries can be configured in the switch.

Example: Configuring static ARP for interface VLAN1.

Switch(Config-If-Vlan1)#arp 1.1.1.1 00-03-0f-f0-12-34 eth 1/2

17.3.2.2.2 ip proxy-arp

Command: ip proxy-arp

no ip proxy-arp

Function: Enables proxy ARP for VLAN interface; the "no ip proxy-arp" command disables proxy ARP.

Default: Proxy ARP is disabled by default.

Command mode: VLAN Interface Mode

Usage Guide: When an ARP request is received on the layer 3 interface, requesting an IP address in the same IP segment of the interface but not the same physical network, and the proxy ARP interface has been enabled, the interface will reply to the ARP with its own MAC address and forward the actual packets received. Enabling this function allows machines to physically be separated but in the same IP segment and communicate via the proxy ARP interface as if in the same physical network. Proxy ARP will check the route table to determine whether the destination network is reachable before responding to the ARP request; ARP request will only be responded if the destination is reachable. Note: the ARP request matching default route will not use proxy.

Example: Enabling proxy ARP for VLAN 1.

Switch(Config-If-Vlan1)#ip proxy-arp

17.3.3 ARP Forwarding Troubleshooting Help

17.3.3.1 Monitor and Debug Commands

17.3.3.1.1 show arp

Command: show arp [<*ip-addr*>][<*vlan-id*>][<*hw-addr*>][type {static|dynamic}][count] }

Function: Displays the ARP table.

Parameters: **<*ip-addr*>** is a specified IP address; **<*vlan-id*>** stands for the entry for the identifier of specified VLAN; **<*hw-addr*>** for entry of specified MAC address; "static" for static ARP entry; "dynamic" for dynamic ARP entry; "count" displays number of ARP entries.

Command mode: Admin Mode

Usage Guide: Displays the content of current ARP table such as IP address, MAC address, hardware type, interface name, etc.

Example:

Switch#sh arp

Total arp items: 3, matched: 3, Incomplete: 0

Address	Hardware Addr	Interface	Port	Flag
50.1.1.6	00-0a-eb-51-51-38	Vlan50	Ethernet3/11	Dynamic
50.1.1.9	00-00-00-00-00-09	Vlan50	Ethernet1/1	Static
150.1.1.2	00-00-58-fc-48-9f	Vlan150	Ethernet3/4	Dynamic

Displayed information	Explanation
Total arp items	Total number of Arp entries.
the matched	ARP entry number matching the filter conditions
InCompleted	ARP entries have ARP request sent without ARP reply
Address	IP address of Arp entries
Hardware Address	MAC address of Arp entries
Interface	Layer 3 interface corresponding to the ARP entry.
Port	Physical (Layer2) interface corresponding to the ARP entry.
Flag	Describes whether ARP entry is dynamic or static.

17.3.3.1.2 clear arp-cache

Command: clear arp-cache

Function: Clears arp table.

Parameters: N/A.

Command mode: Admin Mode

Usage Guide: Clears the content of current ARP table, but it does not clear the current static ARP table.

Example:

Switch#clear arp-cache

17.3.3.1.3 debug arp

Command: debug arp

no debug arp

Function: Enables the ARP debugging function; the "**no debug arp**" command disables this debugging function.

Default: ARP debug is disabled by default.

Command mode: Admin Mode

Usage Guide: Display contents for ARP packets received/sent, including type, source and destination address, etc.

Example: Enabling ARP debugging

Switch#debug arp

ip arp debug is on

Switch#%Apr 19 15:59:42 2005 IP ARP: rcvd, type 1, src 192.168.2.100, 000A.EB5B.

780C, dst 192.168.2.1, 0000.0000.0000 flag 0x0.

%Apr 19 15:59:42 2005 IP ARP: sent, type 2, src 192.168.2.1, 0003.0F02.310A, dst

192.168.2.100, 000A.EB5B.780C.

17.3.3.2 ARP Troubleshooting Help

If ping from the switch to directly connected network devices fails, the following can be used to check the possible cause and create a solution.

- Check whether the corresponding ARP has been learned by the switch.
- If ARP has not learned, then enabled ARP debugging information and view sending/receiving condition of ARP packets.
- Defective cable is a common cause of ARP problems and may disable ARP learning.

17.4 Web management

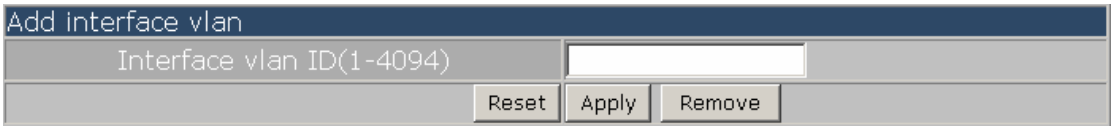
Click “L3 forward configuration” to enter L3 forward allocation root node in the content on the left of the root page.

- Click “L3 interface configuration” to enter L3 port related configuration
- Click “IP route Aggregate configuration” to enter IP routing aggregate configuration
- Click “ARP configuration” to enter ARP related configuration

17.4.1 L3 port configuration

Click “Add interface vlan” in L3 port configuration to create/delete L3 ports. This is equivalent to CLI command 17.1.2.2.1

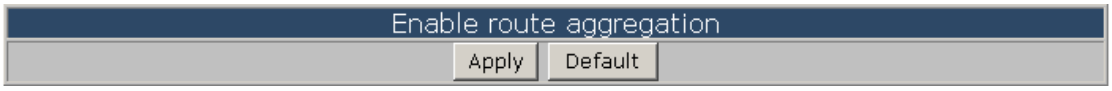
- VlanID: VLAN ID
- Apply: create a L3 port by specified VLAN ID
- Remove: delete a L3 port by specified VLAN ID



17.4.2 IP route aggregation configuration

Click “Route aggregate configuration” in IP route aggregate mode to make configurations. It equals to CLI command 17.2.2.2.1:

- Apply: enable IP route aggregation
- Default: disable IP route aggregation



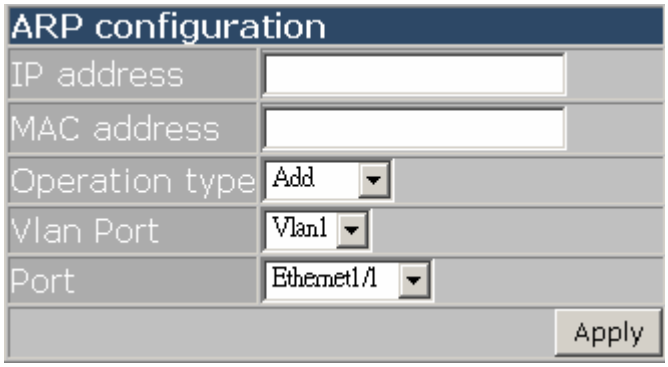
17.4.3 ARP configuration

Users can configure ARP, Proxy ARP, clear dynamic ARP, check ARP items, etc. in ARP related configuration.

17.4.3.1 Configure static ARP

Click “ARP configuration” to configure static ARP. Equivalent to CLI command 17.3.2.2.1:

- IP address: specifies the IP address of related static ARP
- MAC address: specifies the MAC address of related static ARP
- Operation type: Add means to add a static ARP item; Remove means to delete a static ARP item (selected from scroll bar menu)
- Vlan Port: specifies the L3 port of static AP (selected from the drop down menu)
- Port: Specifies the L2 port of static ARP (selected from the drop down menu)



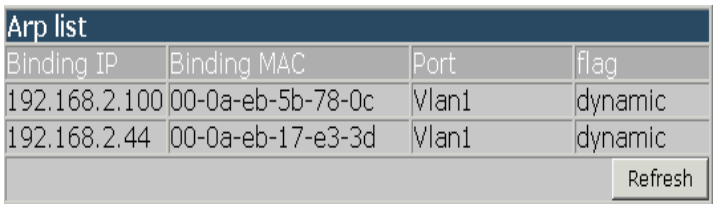
17.4.3.2 Clear ARP

Click “Clear ARP cache” to delete all dynamic ARP items. Equivalent to CLI command 17.3.2.2.3:

- Apply: deletes all dynamic ARP

17.4.3.3 Show ARP

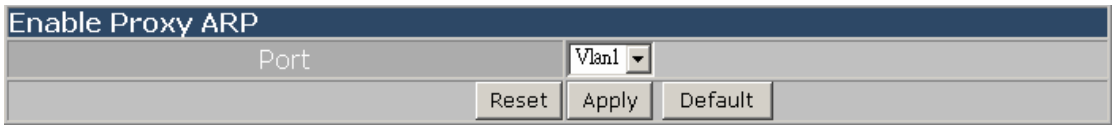
Click “Show ARP” to display all ARP items. No parameter is required. Equivalent to CLI command 17.3.3.1.1



17.4.3.4 Proxy ARP configuration

Click “Proxy ARP configuration” to setup Proxy ARP. Equals to CLI command 17.3.2.2.2:

- Port: specifies the L3 port to setup Proxy ARP (selected from the drop down menu)
- Apply: enables Proxy ARP
- Default: disables Proxy ARP



Chapter 18 Routing Protocol Configuration

To communicate with a remote host over the Internet, a host must choose a proper route via a set of routers/L3 switches.

Both routers and layer 3 switches calculate the route using CPU. The difference is that layer 3 switches add the calculated route in the switch chip and forward using the chip at wire speed. Routers always store the calculated route in the route table or route buffer, and data forwarding is performed by the CPU. For this reason, although both routers and switches can perform route selection, layer 3 switches have greater advantage over routers in data forwarding. ES4704BD is a layer 3 switch launched by Edge-Core that follows the described basic theories and methods used in layer 3 switch route selection.

In route selection, the responsibility of each layer 3 switch is to select a proper midway route according to the destination of the packet received; and then send the packet to the next layer 3 switch until the last layer 3 switch in the route sends the packet to the destination host. A route is the path selected by each layer 3 switch to pass the packet to the next layer 3 switch. A route can be grouped into direct route, static route and dynamic route.

A Direct route refers to a path that directly connects to a layer 3 switch, and can be obtained with no calculation.

A Static route is a manually specified path to a network or a host; static route cannot be changed freely. Static route is simple and consistent, and can limit illegal route modification, and is convenient for load balance and route backup. However, as this is set manually, it is not suitable for mid to large scale networks where routes are too huge and complex.

A Dynamic route is the path to a network or a host calculated by the layer 3 switch according to the routing protocols enabled. If the next hop layer 3 switch in the path is not reachable, layer 3 switch will automatically discard the path to that next hop layer 3 switch and choose the path through other layer 3 switches.

There are two dynamic routing protocols: Interior Gateway Protocol (IGP) and Exterior Gateway protocol (EGP). IGP is the protocol used to calculate the route to a destination inside an autonomous system. IGP is supported by ES4704BD and includes routing protocols like RIP and OSPF. RIP and OSRF can be configured according to the requirement. ES4704BD supports running several IGP dynamic routing protocols at the same time. Or, other dynamic routing protocols and static route can be introduced in a dynamic routing protocol, so that multiple routing protocols can be associated.

18.1 Route Table

As mentioned before, layer 3 switches are mainly used to establish the route from the current layer 3 switch to a network or a host, and to forward packets according to route. Each layer 3 switch has its own route table containing all routes used by that switch. Each route entry in the route table specifies the VLAN interface that should be used for forwarding packets to reach a destination host or the next layer 3 switch hop to the host.

The route table mainly consists of the following:

- Destination address: used to identify the destination address or the destination network of a packet.

- Network mask: used together with destination address to identify the destination host or the segment that the layer 3 switch resides. Network mask consists of several consecutive binary 1's, and usually in the decimal format (an address consists of 1 to 4 255's) When "AND" the destination address with network mask, we can get the network address for the destination host or the segment that the layer 3 switch resides in. For example, the network address of a host or the segment that the layer 3 switch resides with a destination address of 200.1.1.1 and mask 255.255.255.0 is 200.1.1.0.
- Output interface: specifies the interface of the layer 3 switch to forward IP packets.
- IP address of the next layer 3 switch (next hop): specifies the next layer 3 switch that IP packet will pass.
- Route entry priority: There may be several different next hop routes leading to the same destination. These routes may be discovered by different dynamic routing protocols or static routes manually configured. The entry has the highest priority (smallest value) and becomes the current best route. The user can configure several routes of different priority to the same destination; the layer 3 switch will choose one route for IP packet forwarding according to the priority order.

To avoid too large of a route table, a default route can be set. Once route table lookup fails, the default route will be chosen for forwarding packets.

The table below describes the routing protocols supported by ES4704BD and the default route lookup priority values.

Routing Protocols or route type	Default priority value
Direct route	0
OSPF	110
Static route	1
RIP	120
OSPF ASE	150
IBGP	200
EBGP	20
Unknown route	255

18.2 Static Route

18.2.1 Introduction to Static Route

As mentioned earlier, the static route is the manually specified path to a network or a host. A Static route is simple, consistent and can prevent illegal route modification. It is convenient for load balance and route backup, but also has its own defects. Static route, as its name indicates, is static, it won't modify the route automatically on network failure, and manual configuration is required on such occasions, therefore it is not suitable for mid to large-scale networks.

Static route is mainly used for the following two conditions: 1) in stable networks to reduce the load of route selection and routing data streams. For example, static routes can be used in route to STUB network. 2) For route backup, configure static route in the backup line, with a lower priority than the main line.

Static route and dynamic route can coexist; A layer 3 switch will choose the route with the highest priority according to the priority of routing protocols. At same time, static routes can be introduced (redistribute) in dynamic route, and change the priority of the static route introduced.

18.2.2 Introduction to Default Route

Default route is a static route, which is used only when no matching route is found. In the route table, default route in is indicated by a destination address of 0.0.0.0 and a network mask of 0.0.0.0, too. If the route table does not have the destination of a packet and has no default route configured, the packet will be dropped, and ICMP packets will be sent to the source address to indicate the destination address or network is unreachable.

18.2.3 Static Route Configuration

18.2.3.1 Static Route Configuration Task Sequence

1. Static Route Configuration
2. Default Route Configuration

1. Static Route Configuration

Command	Explanation
Global Mode	
ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>] **no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]**	Configures a static route; the "**no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]"** command deletes a static route entry.

2. Default Route Configuration

Command	Explanation
Global Mode	
ip route 0.0.0.0 0.0.0.0 <*gateway*> [<*preference*>] **no ip route 0.0.0.0 0.0.0.0 <*gateway*> [<*preference*>]**	Configures a default route; the "**no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]"** command deletes a default route entry.

18.2.3.2 Static Route Configuration Commands

- **ip route**
- **show ip route**

18.2.3.2.1 ip route

Command: ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]

no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]

Function: Configures a static route; the "**no ip route <*ip_address*> <*mask*> <*gateway*> [<*preference*>]"** command deletes a static route entry.

Parameters: <***ip-address***> and <***mask***> are the IP address and subnet mask, in decimal format;

<*gateway*> is the IP address for the next hop in decimal format; **<*preference*>** is the route priority, ranging from 1 to 255, the smaller preference indicates higher priority.

Default: The default priority for static route of ES4704BD is 1.

Command mode: Global Mode

Usage Guide: When configuring the next hop for static route, next hop IP address can be specified for routing packets.

The default preference of all route type in ES4704BD is listed below:

Route Type	Preference Value
Direct route	0
Static Route	1
OSPF	110
RIP	120
IBEP	200
EBGP	20

By default, a direct route has the highest priority, and static route, EBGP, OSPF, RIP and IBGP have descending priorities in the order listed.

Example:

Example 1: adding a static route

Switch(Config)#ip route 1.1.1.0 255.255.255.0 2.1.1.1

Example 2: adding a default route

Switch(Config)#ip route 0.0.0.0 0.0.0.0 2.2.2.1

18.2.3.2.2 show ip route

Command: show ip route [dest <*destination*>] [mask <*destMask*>] [nextHop <*nextHopValue*>] [protocol {connected | static | rip| ospf | ospf_ase | bgp | dvmrp}] [<*vlan-id*>] [preference <*pref*>] [count]

Function: Displays the route table.

Parameters: **<*destination*>** is the destination network address; **<*destMask*>** is the mask for destination network; **<*nextHopValue*>** stands for the IP address of next hop; **connected** for direct route; **static** for static route; **rip** for RIP route; **ospf** for OSPF route; **ospf_ase** for route introduced by OSPF; **ospf_asebgp** for BGP route; **bgpdvmrp** for DVMRP route; **<*vlan-id*>** for VLAN identifier; **<*pref*>** for router priority, ranging from 0 to 255; **count** displays the number of IP route table entries.

Command mode: Admin Mode

Usage Guide: Displays the content of core route table including: route type, destination network, mask, next hop address, interface, etc.

Example:

Switch#show ip route

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan2	0
C	4.4.4.0	255.255.255.0	0.0.0.0	vlan4	0
S	6.6.6.0	255.255.255.0	9.9.9.9	vlan9	1
R	7.7.7.0	255.255.255.0	8.8.8.8	vlan8	120

Displayed information	Explanation
C - connected	Direct route, the segment directly connects to the layer 3 switch.
S - static	Static route, route are manually configured by the user
R - RIP derived	RIP route, route are obtained through RIP protocol in layer 3 switch
O - OSPF derived	OSPF route, route obtained through OSPF protocol in layer 3 switch
A - OSPF ASE	Route introduced by OSPF
B - BGP derived	BGP route, the route obtained through BGP protocol.
Destination	destination network
Mask	Mask of the destination network
Nexthop	Next hop IP address
Interface	The layer 3 switch interface to next hop.
Pref	Route priority, if another route types exists to the destination network, only the route of the higher priority will be displayed in the core route table.

18.2.4 Configuration Scenario

The figure below is a simple network consisting of three ES4704BD layer 3 switches, the network mask for all switches and PC IP addresses is 255.255.255.0. PC1 and PC3 are connected via the static route set in Swtich1 and Switch3; PC3 and PC2 are connected via the static route set in Switch 3 to Switch 2; PC 1 and PC3 is connected via the default route set in Switch2.

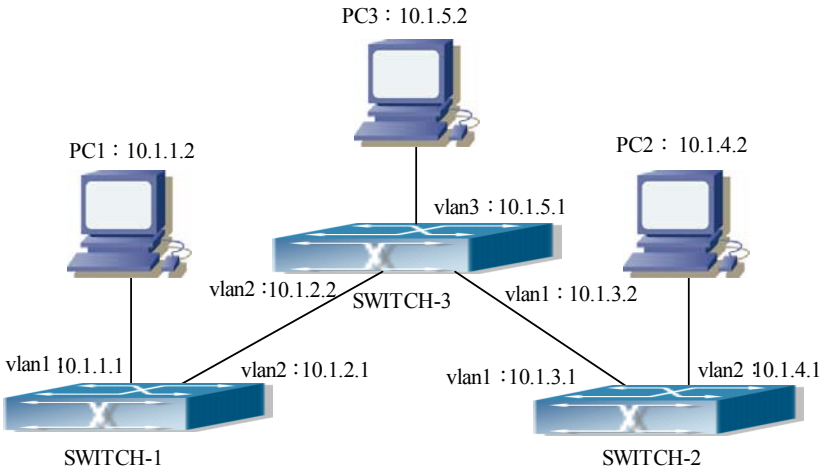


Fig 18-1 Static Route Configurations

Configuration steps:

Configuration of layer 3 switch Switch-1

Switch#config

Switch(Config)#ip route 10.1.5.0 255.255.255.0 10.1.2.2

Configuration of layer3 switch Switch-3

Switch#config

！Next hop use the partner IP address

Switch(Config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1

！Next hop use the partner IP address

Switch(Config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1

Configuration of layer 3 switch Switch-2

Switch#config

Switch(Config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2

This way, ping connectivity can be established between PC1 and PC3, and PC2 and PC3

18.2.5 Troubleshooting Help

18.2.5.1 Monitor and Debug Commands

Command	Explanation
Admin Mode	
show ip route	Displays the content of route table including: route type, destination network, mask, next hop address, and interface, etc.

Uses the “show ip route” command to display the information about static route in the route table: destination IP address, network mask, next hop IP address, forwarding interface, etc.

For example:

Switch#show ip route

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan1	0
S	6.6.6.0	255.255.255.0	2.2.2.9	vlan1	1

S stands for static route, i.e., the static route with the destination network address of 6.6.6.0, network mask of 255.255.255.0, the next hop address of 2.2.2.9 and the forwarding interface of Ethernet vlan1. The priority value of this route is 1.

18.3 RIP

18.3.1 Introduction to RIP

RIP was first introduced in ARPANET, a protocol dedicated to small, simple networks. RIP is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send 2 kinds of information to the neighboring devices regularly:

- Number of hops to reach the destination network, or metrics to use or number of networks to pass.
- What is the next hop, or the director (vector) to use to reach the destination network.

Distance vector layer 3 switches send all their route selecting tables to neighboring layer 3 switches at regular interval. A layer 3 switch will build their own route selecting information table based on the information they receive from neighboring layer 3 switches. Then, it will send this information to its own neighbor layer 3 switches. As a result, the route selection table is built on second hand information. Route beyond 15 hops will be deemed as unreachable.

RIP is a optional routing protocol based on UDP. Hosts using RIP send and receive packets on UDP port 520. All layer 3 switches running RIP send their route table to all neighboring layer 3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer 3 switch will be kept in the route table for another 120 seconds before deletion.

As layer 3 switches use RIP built route table with second hand information, an infinite count may occur. For a network running RIP routing protocol, when an RIP route becomes unreachable, the neighboring RIP layer 3 switch will not send routing update packets at once, instead, it waits until the update interval times out (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, “infinite count” will result. In other words, the route of unreachable layer 3

switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To avoid “infinite count”, RIP provides a mechanism such as “split horizon” and “triggered update” to solve route loop. “Split horizon” is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: “simple split horizon” and “poison reverse split horizon”. Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the above-mentioned routes, but sets the costs of those routes to infinite. “Triggering update” mechanism defines whenever route metric are changed by the gateway, the gateway will advertise the update packets immediately, regardless of the 30 second update timer status.

There are two versions of RIP, version 1 and version 2. RFC1058 introduces RIP-I protocol, RFC2453 introduces RIP-II, which is compatible with RFC1723 and RFC1388. RIP-I updates packets by packets advertisement, subnet mask and authentication are not supported. Some fields in the RIP-I packets are not used and are required to be all 0’s; for this reason, such all 0's fields should be checked when using RIP-I. RIP-I packets should be discarded if such fields are non-zero. RIP-II is a more improved version than RIP-I. RIP-II sends route update packets by use of multicast (multicast address is 224.0.0.9). Subnet mask field and RIP authentication filed (simple plaintext password and MD5 password authentication are supported), and support variable length subnet mask. RIP-II uses some of the zero field of RIP-I and requires no zero field verification. ES4704BD layer 3 switches by default send RIP-II packets by multicast. Both RIP-I and RIP-II packets are accepted.

Each layer 3 switch running RIP has a route database, which contains all route entries for reachable destinations, the route table is built based on this database. When a RIP layer 3 switch sends route update packets to neighboring devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer 3 switch is quite large, causing degradation of network performance.

Besides the above-mentioned, RIP protocol allows route information discovered by the other routing protocols to be introduced into the route table.

The operation of RIP protocol is shown below:

1. Enable RIP. The switch sends request packets to the neighboring layer 3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.
2. The Layer 3 switch modifies its local route table upon receiving the reply packets and sends triggered update packets to the neighboring devices to advertise the route update information. On receiving the triggered update packet, the neighboring layer 3 switches sends triggered update packets to their neighboring layer 3 switches. After a sequence of triggered updates by packet broadcast, all layer 3 switches get and maintain the latest route information.

In addition, RIP layer 3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighboring devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route for a certain interval (holddown timer interval), it will delete that route.

18.3.2 RIP Configuration

18.3.2.1 RIP Configuration Task Sequence

1. Enable RIP (required)
   (1) Enable/disable RIP module.
   (2) Enable interface to send/receive RIP packets
2. Configure RIP parameters (optional)
   (1) Configure RIP sending mechanism
      a. Configure specified RIP packets transmission address
      b. Configure RIP advertisement
   (2) Configure RIP routing parameters
      a. configure route aggregation
      b. configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)
      c. Enable interface to send/receive additional routing metric of RIP packets
      d. Configure interface authentication mode and password
   (3) Configure other RIP parameters
      a. Configure RIP routing priority
      b. Configure zero field verification for RIP packets
      c. Configure timer for RIP update, timeout and hold-down
3. Configure RIP-I/RIP-II switch
   (1) Configure the RIP version to be used in all ports
   (2) Configure the RIP version to send/receive in all ports
   (3) Configure whether to enable RIP packets sending/receiving for ports
4. Disable RIP

1. Enable RIP

The basic configuration for running RIP on ES4704BD is quite simple. Usually, the user needs only enable RIP and enable sending and receiving of RIP packets, i.e., send and receive RIP packets according to default RIP configuration (ES4704BD sends RIP-II packets and receive RIP-I/RIP-II packets by default). If necessary, the version of RIP packets to send/receive can be switched, sending/receiving RIP packets can be enabled/disabled, see 3 for details.

Command	Explanation
Global Mode	
[no] router rip	Enables RIP; the "**no router rip**" command disables RIP
Interface Mode	
[no] ip rip work	Enables sending/receiving RIP packets on the interface; the "**no ip rip work**" command disables sending/receiving RIP packets on the interface

2. Configure RIP protocol parameters

(1) Configure RIP sending mechanism

a. Configure regular RIP packets transmission

b. Configure RIP advertisement

Command	Explanation
RIP configuration mode	
[no] rip broadcast	Indicates RIP layer 3 switch allows all ports to send broadcast/multicast packets; the "**no rip broadcast**" command disables all ports to send broadcast/multicast packets

2) Configure RIP routing parameters.

a. Configure route aggregation

Command	Explanation
RIP configuration mode	
auto-summary **no auto-summary**	Configures route aggregation; the "**no auto-summary"** command disables route aggregation.

b. configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

Command	Explanation
RIP configuration mode	
default-metric <*value*> **no default-metric**	Sets the default route metric for route to be introduced; the "**no default-metric**" command restores the default setting.
redistribute { static | ospf | bgp} [metric <*value*>] **no redistribute { static | ospf | bgp }**	Introduces static, OSPF or BGP routes to RIP packets; the "**no redistribute { static | ospf | bgp }**" command cancels the introduced routes of specified protocol.

c. Enable interface to send/receive additional routing metric of RIP packets

Command	Explanation
Interface Mode	
ip rip metricout <*value*> **no ip rip metricout**	Sets the additional route metric for route on sending RIP packets from the interface; the "**no ip rip metricout**" command restores the default setting.
ip rip metricin <*value*> **no ip rip metricin**	Sets the additional route metric for route on receiving RIP packets from the interface; the "**no ip rip metricin**" command restores the default setting.

d. Configure interface authentication mode and password

Command	Explanation
Interface Mode	

ip rip authentication mode {text| md5 **type {cisco|usual}}** **no ip rip authentication mode**	Sets the authentication method; the "**no ip rip authentication mode**" command restores the default plain text authentication method.
ip rip authentication key-chain <*name-of-chain*> **no ip rip authentication key-chain**	Sets the authentication key; the "**no ip rip authentication key-chain**" command means no authentication key is used.

3) Configure other RIP parameters

a. Configure RIP routing priority

b. Configure zero field verification for RIP packets

c. Configure timer for RIP update, timeout and hold-down

Command	Explanation
RIP configuration mode	
rip preference <*value*> **no rip preference**	Sets the route priority of RIP; the "**no rip preference**" command restores the default setting.
[no] rip checkzero	Enables zero fields verification to RIP-I packets, refuses to process if non-zero zero field; the "**no rip checkzero**" command cancels this check for zero field
timer basic <*update*> <*invalid*> <*holddown*> **no timer basic**	Adjusts the RIP timers for update, expire, and hold down; the "**no timer basic**" command restores the default settings.

3. Configure RIP-I/RIP-II switch

(1) Configure the RIP version to be used in all ports

Command	Explanation
RIP configuration mode	
version { 1 | 2 } **no version**	Sets the version of RIP packets to send/receive on all ports; the "**no version**" command restores the default, i.e., sends v2 packets, receives both v1 and v2 packets

(2) Configure the RIP version to send/receive in all ports

(3) Configure whether to enable RIP packets sending/receiving for ports

Command	Explanation
Interface Mode	
ip rip send version { v1 | v2 [bc|mc] } **no ip rip send version**	Sets the version of RIP packets to send on all ports; the "**no ip rip send version**" command restores the default, i.e., send v2 packets,

ip rip receive version {v1 | v2 | v12} **no ip rip receive version**	Sets the version of RIP packets to receive on all ports; the "**no ip rip receive version**" command restores the default, i.e., receives both v1 and v2 packets,
[no] ip rip input	Enables receiving RIP packets on the interface; the "**no ip rip input**" command disables receiving RIP packets on the interface
[no] ip rip output	Enables sending RIP packets on the interface; the "**no ip rip output**" command disables sending RIP packets on the interface

4. Disable RIP

Command	Explanation
Global Mode	
no router rip	Disables RIP

RIP (Routing Information Protocol) is a dynamic interior routing protocol based on distance vector. It is widely used for its simple configurations. RIP exchanges routing information by UDP packet advertisement, route update information is sent every 30 seconds. It uses hop number as the standard for choosing a route, routes with less hops to the same destination network will be chosen first. The maximum hop number allowed is 16, so RIP is suitable for autonomous systems with relative small diameter. RIP configuration commands are mainly used in Global Mode, RIP configuration mode, Interface Mode and Admin Mode.

18.3.2.2 RIP Configuration Commands

- **auto-summary**
- **default-metric**
- **ip rip authentication key-chain**
- **ip rip authentication mode**
- **ip rip metricin**
- **ip rip metricout**
- **ip rip input**
- **ip rip output**
- **ip rip receive version**
- **ip rip send version**
- **ip rip work**
- **ip split horizon**
- **redistribute**
- **rip broadcast**
- **rip checkzero**
- **rip preference**
- **router rip**
- **timer basic**
- **version**
- **show ip protocols**

- **show ip rip**
- **debug ip rip packet**
- **debug ip rip recv**
- **debug ip rip send**

18.3.2.2.1 auto-summary

Command: auto-summary

no auto-summary

Function: Configures route aggregation; the "**no auto-summary"** command disables route aggregation.

Parameters: N/A.

Default: Auto route aggregation is not used by default.

Command mode: RIP configuration mode

Usage Guide: Route aggregation reduces the amount of routing information in the route table and amount of information to be exchanged. RIP-I does not support subnet mask, forwarding subnet route may result in ambiguity. For this reason, route aggregation is always enabled for RIP-I. If you are using RIP-II, you can use "no auto-summary" command to disable route aggregation. If subnet route needs to be broadcasted, route aggregation can also be disabled.

Example: Setting the RIP version to RIP-II and disables route aggregation.

Switch(Config)#router rip

Switch(Config-Router-Rip)#version 2

Switch(Config-Router-Rip)#no auto-summary

Related command: version

18.3.2.2.2 default-metric

Command: default-metric <*value*>

no default-metric

Function: Sets the default route metric for route to be introduced; the "**no default-metric**" command restores the default setting.

Parameters: < *value*> is the value of route metric, ranging from 1 to 16.

Default: The default route metric is 1.

Command mode: RIP configuration mode

Usage Guide: "**default-metric**" command sets the default route metric used in introducing routes from the other routing protocols to RIP. When using "**redistribute**" command to introduce routes of the other protocols without specifying a detailed route metric, the default route metric set by "**default-metric**" command applies.

Example: Sets the default route metric for introducing routes of the other protocols into RIP to 3.

Switch(Config-router-rip)#default-metric 3

Related command: redistribute

18.3.2.2.3 ip rip authentication key-chain

Command: ip rip authentication key-chain <*name-of-chain*>

no ip rip authentication key-chain

Function: Specifies the key to use for RIP authentication; the "**no ip rip authentication key-chain**" command cancels the RIP authentication.

Parameters: <*name-of-chain*> is a string, up to 16 characters are allowed.

Default: RIP authentication is disabled by default.

Command mode: Interface Mode

Usage Guide: Instead of deleting the RIP authentication key, the "**no ip rip authentication key-chain**" command cancels the RIP authentication.

Related command: ip rip authentication

18.3.2.2.4 ip rip authentication mode

Command: ip rip authentiaction mode {text|md5 type {cisco|usual}}

no ip rip authentication mode

Function: Sets the authentication method; the "**no ip rip authentication mode**" command restores the default plain text authentication method.

Parameters: "**text**" for text authentication; "**md5**" for MD5 authentication. There two MD5 authentication methods, Cisco MD5 and conventional MD5.

Default: The default setting is text authentication.

Command mode: Interface Mode

Usage Guide: RIP-I does not support authentication, RIP-II supports 2 authentication methods: text authentication (Simple authentication) and packets authentication (MD5 authentication). There 2 packets types used in MD5 authentication, one format complies with RFC1723 (RIP Version 2 Carrying Additional Information) and the other format conforms to RFC2082 (RIP-II MD5 Authentication).

Example: Setting Cisco MD5 authentication on interface vlan1, the authentication key is "edgecore".

Switch(Config-If-Vlan1)#ip rip authentication mode md5 type cisco

Switch(Config-If-Vlan1)#ip rip authentication key-chain edgecore

Related command: ip rip authentication key-chain

18.3.2.2.5 ip rip metricin

Command: ip rip metricin <*value*>

no ip rip metricin

Function: Sets the additional route metric receiving RIP packets on the interface; the "**no ip rip metricin**" command restores the default setting.

Parameters: < *value*> is the additional route metric, ranging from 1 to 15.

Default: The default additional route metric used for RIP to receive packets is 1.

Command mode: Interface Mode
Related command: ip rip metricout

18.3.2.2.6 ip rip metricout

Command: ip rip metricout <*value*>
no ip rip metricout
Function: Sets the additional route weight sending RIP packets on the interface; the "**no ip rip metricout**" command restores the default setting.
Parameters: < *value*> is the additional route metric, ranging from 0 to 15.
Default: The default additional route metric used for RIP to send packets is 0.
Command mode: Interface Mode
Example: Setting vlan1 interface on the additional route metric of receiving RIP packets to 5, and sending RIP packets to 3.
Switch(Config-If-Vlan1)#ip rip metricin 5
Switch(Config-If-Vlan1)#ip rip metricout 3
Related command: ip rip metricin

18.3.2.2.7 ip rip input

Command: ip rip input
no ip rip input
Function: Enables receiving RIP packets on the interface; the "**no ip rip input**" command disables receiving RIP packets on the interface
Default: Receiving RIP packet is enabled by default.
Command mode: Interface Mode
Usage Guide: This command is used with the other two commands "**ip rip output**" and "**ip rip work**", "**ip rip work**" is equal to "**ip rip input**" & "**ip rip output**" in function, the latter two commands control the receiving and sending of RIP packet on the interface, the former equals the total of the latter two commands.
Related command: ip rip output

18.3.2.2.8 ip rip output

Command: ip rip output
no ip rip output
Function: Enables sending RIP packets on the interface; the "**no ip rip output**" command disables sending RIP packets on the interface
Default: Sending RIP packet is enabled by default.
Command mode: Interface Mode
Usage Guide: This command is used with two other commands: "**ip rip output**" and "**ip rip work**". "**ip rip work**" is equal to "**ip rip input**" & "**ip rip output**" in function, the latter two commands control the receiving and sending of RIP packet on the interface, the former equals the total of the latter two commands.

Related command: ip rip input

18.3.2.2.9 ip rip receive version

Command: ip rip receive version {v1 | v2 | v12}

no ip rip receive version

Function: Configure the RIP version to receive on the interface. The default setting is to receive both RIP v1 and v2 packets; the "**no ip rip receive version**" command restores the default setting.

Parameters: v1 and **v2** stands for RIP version1 and RIP version 2 respectively, **v12** stands for both RIP version 1 and 2.

Default: The default setting is **v12**, i.e., accept both RIP version 1 and version 2 packets.

Command mode: Interface Mode

18.3.2.2.10 ip rip send version

Command: ip rip send version { v1 | v2 [bc|mc] }

no ip rip send version

Function: Configures RIP version to send on the interface; the "**no ip rip send version**" command restores the default setting.

Parameters: v1 | v2 are both RIP version numbers; **[bc|mc]** is configured only for RIP-II for specifying the sending method, **BC** for broadcast, **MC** for multicast. When configured to send RIP-II packets, the interface sends RIP-II packets by **MC** (multicast) by default, packets are only broadcasted when **BC** is set on the interface.

Default: RIP-II packets are sent by default.

Command mode: Interface Mode

Usage Guide: When configured to send RIP-II packets, the interface sends RIP-II packets in **MC** (multicast) by default, packets are only broadcasted when **BC** is set on the interface.

18.3.2.2.11 ip rip work

Command: ip rip work

no ip rip work

Function: Configures the interface to run RIP or not; the "**no ip rip work**" command disables RIP packet sending/receiving on the interface.

Default: After enabling RIP, RIP is enabled on the ports by default.

Command mode: Interface Mode

Usage Guide: This command is equal to "**ip rip input**" & "**ip rip output**" in function, the latter two commands control the receiving and sending of RIP packets on the interface, the former equals the total of the latter two commands.

Related command: ip rip input, ip rip output

18.3.2.2.12 ip split-horizon

Command: ip split-horizon

no ip split-horizon

Function: Enables split horizon; the "**no ip split-horizon**" command disables split horizon.

Default: Split horizon is enabled by default.

Command mode: Interface Mode

Usage Guide: Sets split horizon to prevent routing loops, i.e., prevent layer 3 switches from broadcasting the route leaned from the same interface.

Example: Disabling split horizon for interface vlan1.

Switch(Config)#interface vlan1

Switch(Config-If-Vlan1)#no ip split-horizon

18.3.2.2.13 redistribute

Command: redistribute { static | ospf | bgp} [metric <*value*>]

no redistribute { static | ospf | bgp }

Function: Introduces routes of the other protocols into RIP; the "**no redistribute { static | ospf | bgp }**" command cancels the introduction.

Parameters: static specifies static routes to be introduced; **ospf** for OSPF routes; **bgp** for BGP routes; **<*value*>** stands for the route metric in introducing the routes, ranging from 1 to 16.

Default: Other routes are not introduced to RIP by default. If routes of the other routing protocols are introduced without metric value, the default metric value is used.

Command mode: RIP configuration Mode

Usage Guide: Use this command to introduce routes of other routing protocols as RIP routes to improve RIP performance.

Example: Setting the route metric of OSPF route to 5, and static route metric to 8.

Switch(Config-Router-Rip)#redistribute ospf metric 5

Switch(Config-Router-Rip)#redistribute static metric 8

18.3.2.2.14 rip broadcast

Command: rip broadcast

no rip broadcast

Function: Configures RIP layer 3 switch to allow all ports to send broadcast/multicast packets; the "**no rip broadcast**" command disables all ports to send broadcast/multicast packets, instead, only neighboring layer 3 switches can exchange RIP packets.

Default: RIP broadcast packets are sent by default.

Command mode: RIP configuration Mode

18.3.2.2.15 rip checkzero

Command: rip checkzero

no rip checkzero

Function: Use this command to check the zero fields of RIP-I packets, the "**no rip**

checkzero“ command cancel this check for zero field. Since there are no zero fields in RIP-II packets, this command has no effect on RIP-II packets.

Default: Zero fields are check in RIP-I packets by default.

Command mode: RIP configuration mode

Usage Guide: RIP-I packet must have zero field, this command can be used to enable/disable check for RIP-I packet zero field. If non-zero zero field found in RIP-I packet, that RIP-I packet will be discarded.

Example: Disabling zero field check for RIP-I packets.

Switch(Config-router-rip)#no ip checkzero

18.3.2.2.16 rip preference

Command: rip preference <*value*>

no rip preference

Function: Sets the route priority of RIP; the “**no rip preference**” command restores the default setting.

Parameters: < *value*> is the priority value, ranging from 0 to 255.

Default: The default RIP priority is 120.

Command mode: RIP configuration mode

Usage Guide: Each routing protocol has its own priority, the value of which is decided by the specific routing policy. The priority determines the best route of what routing protocol will be the route in the core route table. This command can be used to manually adjust RIP priority; the adjustment will apply to new routes. Due to the nature of RIP, the RIP priority should not be set too high.

Example: Setting the RIP priority to 10.

Switch(Config-router-rip)#rip prefenrence 10

18.3.2.2.17 router rip

Command: router rip

no router rip

Function: Enables RIP and enters RIP configuration mode; the “**no router rip**” command disables RIP.

Default: RIP is disabled by default.

Command mode: Global Mode

Usage Guide: This command enables switch for RIP, it must be run before other configurations to RIP can be made.

Example: Enabling RIP configuration mode

Switch(Config)#router rip

Switch(Config-Router-Rip)#

18.3.2.2.18 timer basic

Command: timer basic <*update*> <*invalid*> <*holddown*>

no timer basic

Function: Adjusts the time of RIP timers for update, expire, and hold down; the "**no timer basic**" command restores the default setting.

Parameter <*update*> stands for the interval in seconds to send update packets, ranging from 1 to 2,147,483,647; **<*invalid*>** for the interval in seconds to declare a RIP route invalid, ranging from 1 to 2,147,483,647; **<*holddown*>** for the interval in seconds to keep a RIP route after it is declared to be invalid, ranging from 1 to 2,147,483,647.

Default: The default value for **<*update*>** is 30; 180 for **<*invalid*>**; and 120 for <***holddown***>.

Command mode: RIP configuration mode

Usage Guide: The system advertises RIP update packets every 30 seconds by default. If no update packet from a route is received after 180 seconds, that route is considered to be invalid. However, the route will be kept in the route table for another 120 seconds and will be deleted after that. It should be noted in adjusting RIP time out timers that the time to declare invalid route should be at least greater than RIP update time, and the holddown time should also be greater than RIP update interval and must be integer multiples of the RIP update interval.

Example: Setting the RIP route table update time to 20 seconds, time to declare invalid to 80 seconds, and time to delete entry to 60 seconds.

Switch(Config-Router-Rip)#timer basic 20 80 60

18.3.2.2.19 version

Command: version {1| 2}

no version

Function: Configures the RIP version to send/receive on all ports; the "**no version**" command restores the default setting.

Parameters: 1 for RIP version 1, 2 for RIP version 2.

Default: The default setting sends RIP-I packets and receives both RIP-I and RIP-II packets.

Command mode: RIP configuration mode

Usage Guide: 1 means all ports only send/accept RIP-I packets, 2 for send/accept RIP-II packets only. The default setting sends RIP-I packets and receives both RIP-I and RIP-II packets.

Example: Setting the interface to send/receive RIP-II packets.

Switch(Config-router-rip)#version 2

Related command: ip rip receive version

ip rip send version

18.3.2.2.20 show ip protocols

Command: show ip protocols

Function: Displays the information of the routing protocols running in the switch.

Command mode: Admin Mode

Usage Guide: The user can decide whether the routing protocols configured are correct and perform routing troubleshooting according to the output of this command.

Example:

Switch#sh ip protocols

RIP information

rip is turning on

default metrict 16

neighbour is:NULL

preference is 100

rip version information is:

interface	send version	receive version
vlan2	V2BC	V12
vlan3	V2BC	V12
vlan4	V2BC	V12

Displayed information	Explanation
RIP is turning on	The running routing protocol is RIP
default metric	RIP protocol default metric value
neighbour is:	The neighbor layer 3 switch connecting to this RIP switch
Preference	RIP routing priority
rip version information	Displays the version information for RIP, including the RIP version of sending (V1 for RIP-I, V2 for RIP-II), RIP sending method (BC for broadcast, MC for multicast), RIP version of receiving (V1 for RIP-I, V2 for RIP-II, V12 for both RIP-I and RIP-II)

18.3.2.2.21 show ip rip

Command: show ip rip

Function: Displays the current running status and configuration information for RIP.

Command mode: Admin Mode

Usage Guide: The user can check the default metric of RIP route. The specified sending destination address and metric value according to the output of this command will be shown.

Example:

Switch#sh ip rip
RIP information
rip is turning on
default metric 16
neighbour is
preference is 100

Displayed information	Explanation
rip is turning on	RIP routing is enabled
default metric 16	The default metric for introduced route is 16

neighbour is	The specified destination address
preference is 100	RIP routing priority is 100

18.3.2.2.22 debug ip rip packet

Command: debug ip rip packet
no debug ip rip packet

Function: Enables the RIP packet debugging function for sending/receiving: the **"no debug IP packet"** command disables this debugging function.

Default: Debugging is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug ip rip pa
"debug ip rip pa" executed successfully.
00：04：20：

start at 260**********
send packets to 11.11.11.2
packet header： cmd： response, version： 1
no. dest dest_mask gatedway metric
1： 159.226.0.0 0.0.0.0 0.0.0.0 1
00：04：20：

start at 260**********
send packets to 159.226.255.255
packet header： cmd： response, version： 1
no. dest dest_mask gatedway metric
1： 159.222.0.0 0.0.0.0 0.0.0.0 2

2： 11.11.11.2 0.0.0.0 0.0.0.0 2

00：04：20：

start at 260**********

received a rip packet from 159.226.42.1

rip packet cmd ： 2 version：1

18.3.2.2.23 debug ip rip recv

Command: debug ip rip recv

no debug ip rip recv

Function: Enables the RIP packet debug function for receiving: the "**no debug ip rip recv**" command disables the debug function.

Default: Debug is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug ip rip rec

start at 230**********

received a rip packet from 159.226.42.1

rip packet cmd ： 2 version：1

00：03：59：

start at 238**********

received a rip packet from 11.11.11.2

rip packet cmd ： 2 version：1

00：03：59：

rip receive response

packet head 14872964; packet end 14872984

recv packets from 11.11.11.2

packet header： cmd： response, version： 1

no. dest dest_mask gatedway metric

1： 159.222.0.0 0.0.0.0 0.0.0.0 1

18.3.2.2.24 debug ip rip send

Command: debug ip rip send

no debug ip rip send

Function: Enables the RIP packet debug function for sending: the "**no debug ip rip send**"

command disables the debug function.

Default: Debugging is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug ip rip send

00：02：50：

start at 170**********

send packets to 11.11.11.2

packet header： cmd： response, version： 1

no.	dest	dest_mask	gatedway	metric
1：	159.226.0.0	0.0.0.0	0.0.0.0	1

00：02：50：

start at 170**********

send packets to 159.226.255.255

packet header： cmd： response, version： 1

no.	dest	dest_mask	gatedway	metric
1：	159.222.0.0	0.0.0.0	0.0.0.0	2
2：	11.11.11.2	0.0.0.0	0.0.0.0	2

18.3.3 Typical RIP Scenario

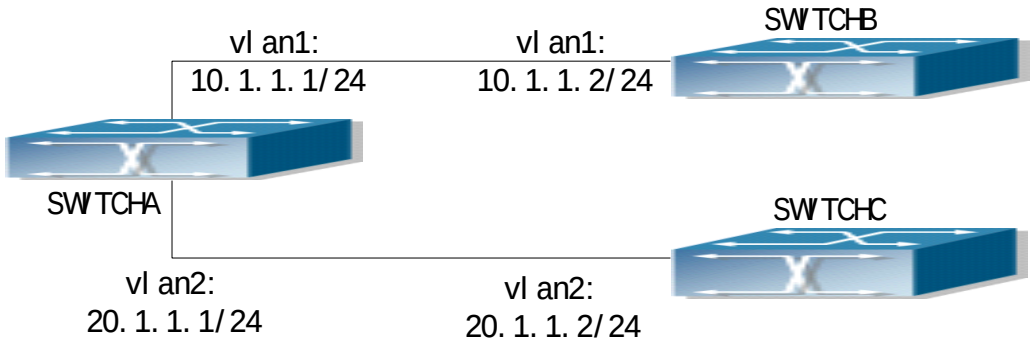


Fig 18-2 RIP Scenario

As shown in the figure a network consists of three layer 3 switches. SwitchA and SwitchB connect to SwitchC through interface vlan1 and vlan2. All the three switches are running RIP. Assume SwitchA vlan1(10.1.1.1) and vlan2 (20.1.1.1) exchange update information with SwitchB vlan1 (10.1.1.2) only, update information is not exchanged between switchA and switchC vlan2 (20.1.1.2). The configuration for SwitchA, SwitchB and SwitchC is shown below:

a) Configuration of layer 3 switch SwitchA

!Configuration of the IP address for interface vlan1

SwitchA#config

SwitchA(Config)# interface vlan 1

SwitchA(Config-If-Vlan1)# ip address 10.1.1.1 255.255.255.0

SwitchA (Config-If-vlan1)#exit

!Configuration of the IP address for interface vlan2

SwitchA(Config)# interface vlan 2

SwitchA(Config-If-vlan2)# ip address 20.1.1.1 255.255.255.0

！Enable RIP

SwitchA(Config)#router rip

SwitchA(Config-router-rip)#exit

！Enable vlan1 to send/receive RIP packets

SwitchA(Config)#interface vlan 1

SwitchA(Config-If-vlan1)#ip rip work

SwitchA(Config-If-vlan1)#exit

！Enable vlan2 to send/receive RIP packets

SwitchA (Config-If-vlan2)# ip rip work

SwitchA (Config-If-vlan2)#exit

SwitchA(Config)#exit

SwitchA#

b) Configuration of layer 3 switch SwitchB

!Configuration of the IP address for interface vlan1

SwitchB#config

SwitchB(Config)# interface vlan 1

SwitchB(Config-If-vlan1)# ip address 10.1.1.2 255.255.255.0

SwitchB (Config-If-vlan1)exit

！Enable RIP and configure the IP address for the neighbor layer3 switch

SwitchB(Config)#router rip

SwitchB(Config-router-rip)#exit

！Enable vlan1 to send/receive RIP packets

SwitchB(Config)#interface vlan 1

SwitchB (Config-If-vlan1)#ip rip work

SwitchB (Config-If-vlan1)#exit

SwitchB(Config)#exit

SwitchB#

c) Configuration of layer 3 switch SwitchC

!Configuration of the IP address for interface vlan2

SwitchC#config

SwitchC(Config)# interface vlan 2

SwitchC(Config-If-vlan2)# ip address 20.1.1.2 255.255.255.0

SwitchC (c config-If-vlan2)#exit

！Enable RIP

```
SwitchC(Config)#router rip
SwitchC(Config-router-rip)#exit
！Enable vlan2 to send/receive RIP packets
SwitchC(Config)#interface vlan 2
SwitchC (Config-If-vlan2)#ip rip work
SwitchC (Config-If-vlan2)exit
SwitchC(Config)#exit
SwitchC#
```

18.3.4 RIP Troubleshooting Help

1. Monitor and Debug Commands
2. RIP Troubleshooting Help

18.3.4.1 Monitor and Debug Commands

Command	Explanation
Admin Mode	
show ip rip	Displays the current running status and configuration information for RIP. The user can decide whether the configurations are correct or not and perform RIP troubleshooting according to the output of this command.
show ip route	Displays route table information, RIP routing information can be checked.
show ip protocols	Displays protocol information
[no] debug ip rip packet	Displays all RIP packets received and sent.
[no] debug ip rip recv	Displays all RIP packets received
[no] debug ip rip send	Displays all RIP packets sent.

（1）show ip rip

Displayed information:

RIP information:

Automatic network summarization is not in effect.

default metric for redistribute is :16

neigbour is :NULL

preference is :100

Explanation to displayed information:

Displayed information	Explanation
Automatic network summarization is not in effect	Disable RIP auto aggregation
default metric for redistribute is :16	The default metric for introduced route is 16.
neigbour is	The specified destination address.

preference is :100	RIP routing priority is 100.

（2）show ip route

The "show ip route" command can be used to display the information about RIP routes in the route table: destination IP addresses, network masks, next hop IP addresses, and forwarding interfaces, etc.

For example, displayed information can be:

Switch#show ip route

Total route items is 2, the matched route items is 2

Codes: C - connected, S - static, R - RIP derived, O - OSPF derived

A - OSPF ASE, B - BGP derived, D - DVMRP derived

	Destination	Mask	Nexthop	Interface	Pref
C	2.2.2.0	255.255.255.0	0.0.0.0	vlan1	0
R	7.7.7.0	255.255.255.0	2.2.2.8	vlan2	100

R stands for RIP route, i.e., the RIP route with the destination network address of 7.7.7.0, network mask of 255.255.255.0, the next hop address of 2.2.2.8 and the forwarding interface of Ethernet vlan2. The priority value of this route is 100.

（3）show ip protocols

"show ip protocols" command can be used to display the information of the routing protocols running in the switch.

For example, displayed information can be:

Switch#sh ip protocols

RIP information:

Automatic network summarization is not in effect.

default metric for redistribute is :16

neigbour is:NULL

preference is :100

RIP version information is:

interface	send version	receive version
vlan1	V2BC	V12
vlan2	V2BC	V12
vlan3	V2BC	V12

Switch#

Displayed information	Explanation
Automatic network summarization is not in effect	Disables RIP auto-aggregation
default metric for redistribute is :	RIP protocol default metric value.
neigbour is:	The neighbor layer 3 switch connecting to this RIP switch.
Preference	RIP routing priority.

RIP version information	Displays the version information for RIP, including the RIP version of sending (V1 for RIP-I, V2 for RIP-II), RIP sending method (BC for broadcast, MC for multicast), RIP version of receiving (V1 for RIP-I, V2 for RIP-II, V12 for both RIP-I and RIP-II).

18.3.4.2 RIP Troubleshooting

In configuring and using RIP, the RIP may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use "show interface" command).
- ✧ Enable RIP (use "router rip" command) first, then configure RIP parameters in the appropriate ports, such as use RIP-I or RIP-II.
- ✧ Next, note the inherit nature of RIP: RIP layer 3 switch sends route table update information to all its neighbor layer 3 switches every 30 seconds. If information from a certain layer 3 switch is not received in 180 seconds, that switch is considered failed or unreachable. The route of that switch will be kept in the route table for another 120 seconds before deleting. As a result, if a RIP route is deleted, wait 300 seconds to ensure the entry to be removed from the route table.

If RIP routing problems persists, please run "debug ip rip" and copy the debug information in 3 minute and send the information to Edge-Core technical service center.

18.4 OSPF

18.4.1 Introduction to OSPF

OSPF is short for Open Shortest Path First. It is an interior dynamic routing protocol for autonomous system based on link-state. The protocol creates a link-state database by exchanging link-state among layer 3 switches, and then uses the Open Shortest Path First algorithm to generate a route table based on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since other hosts on the Internet are not managed by those AS and don't share interior routing information with the layer 3 switches on the Internet.

Each link-state layer 3 switches can provide information about the topology with its neighboring layer 3 switches.

- The segment (link) connecting to the layer 3 switches
- State of the connecting link

Link-state information is flooded throughout the network so that all layer 3 switches can get firsthand information. Link-state layer 3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state layer 3 switches

establish neighborhoods by sending “HELLO” to their neighbors, then link-state advertisements (LSA) will be sent among neighboring layer 3 switches. Neighboring layer 3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as “flooding”. In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide routes. Cost can be assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packets to pass, link bandwidth, current load of the link and can even add metrics by the administrator for better assessment of the link-state.

1) When a link-state layer 3 switch enters a link-state interconnected network, it sends a HELLO packet to get to know its neighbors and establish a neighborhood.

2) The neighbors respond with information about the link they are connecting and the related costs.

3) The originate layer 3 switch uses this information to build its own routing table.

4) Then, as part of the regular update, layer 3 switch send link-state advertisement (LSA) packets to its neighboring layer 3 switches. The LSA include links and related costs of that layer 3 switch.

5) Each neighboring layer 3 switch copies the LSA packet and passes it to the next neighbor (flooding).

6) Since a routing database is not recalculated before the layer 3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is, converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. These advantages release some layer 3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPF protocol include the following. OSPF supports networks of various scales, several hundreds of layer 3 switches can be supported in a OSPF network. Routing topology change can be quickly found and converged. Link-state information is used in shortest path algorithm for route calculation, eliminating endless loop. OSPF divides the autonomous system intro ***areas***, reducing database size, bandwidth occupation and calculation load. (According to the position of layer 3 switches in the autonomous system, they can be grouped as internal switches, edge switches, AS edge switches and backbone switches). OSPF supports load balance and multiple routes to the same destination of equal costs. OSPF supports 4 level routing mechanisms (process routing according to the order of route inside an area, route between areas, first category exterior route and second category exterior route). OSPF support IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPF supports sending packets in multicast.

Each OSPF layer 3 switch maintains a database describing the topology of the whole autonomous system. Each layer 3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with the other OSPF layer 3 switches to formal a link-state database describing the whole autonomous system. Each layer 3 switch builds a shortest path tree rooted in itself according to the link-state database, this tree provide the route to all nodes in an autonomous system. If 2 or more layer 3 switches exist (multi-access to the network), "designated layer 3

switch" and "backup designated layer 3 switch" will be selected. Designated layer 3 switch is responsible for broadcasting link-state of the network. This concept helps the traffic among the switches.

OSPF protocol requires the autonomous system to be divided into areas. That is to divide the autonomous system into 0 field (back field) and non-0 filed. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPF uses four different kinds of routes; they are the route inside the area, route between areas, first category exterior route and second category exterior route, in the order of highest priority to lowest. The route inside an area and between areas describe the internal network structure of an autonomous system, while external routes describe the routing information to destination outside the autonomous system. The first type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, the costs of those routes are fair to the costs of OSPF routes; the second type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, but the costs of those routes are far greater than that of OSPF routes, and OSPF route cost is ignored when calculating route costs.

OSPF areas are centered with the Backbone area, identified as the 0 area, all the other areas must be connected to the 0 area logically, and the 0 area must be online. For this reason, the concept of virtual connection is introduced to the backbone area, so that physically separated areas still have logical connectivity to this area. The configurations of all the layer 3 switches in the same area must be the same.

In conclusion, LSA can only be transferred between neighboring layer 3 switches, OSPF protocol includes 5 types of LSA: router LSA, network LSA, summary LSA to the other areas, general LSA to AS edge switches and exterior AS LSA. They can also be called type1 LSA, type2 LSA, type3 LSA, type4 LSA, and type5 LSA. Router LSA is generated by each layer 3 switch inside an OSPF area, and is sent to all the other neighboring layer 3 switches; network LSA is generated by the specified layer 3 switch in the OSPF area of multi-access network, and is sent to all the other neighboring layer 3 switches. (In order to reduce traffic on layer 3 switches in the multi-access network, "designated layer 3 switch" and "backup designated layer 3 switch" should be selected in the multi-access network, and the network link-state is broadcasted by the designated layer 3 switch); summary LSA is generated by switches in OSPF area edge, and is transferred among area edge layer 3 switches; AS exterior LSA is generated by layer 3 switches on exterior edge of AS, and is transferred throughout the AS.

As to autonomous systems mainly advertises exterior link-state, OSPF allow some areas to be configured as STUB areas to reduce the topology database size. Type4 LSA (ASBR summary LSA) and type5 LSA (AS exterior LSA) are not allowed to flood into/through STUB areas. STUB areas must use the default routes, the layer 3 switches on STUB area edge advertise the default routes to STUB areas by summary LSA, those default routes flood inside STUB only and will not get out of STUB area. Each STUB area has a corresponding default route, the route from a STUB area to AS exterior destination must rely on the defaulted route of that area.

The following outlines OSPF priority route calculation process:

1） Each OSPF-enabled layer 3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer 3 switch generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to the other layer 3 switches through link-state

update (LSU) packets. This way, each layer 3 switch receives LSAs from the other layer 3 switches, and all LSAs combined to the link-state database.

2） Since an LSA is a description to the network topology structure around a layer 3 switch, the LS database is the description to the network topology structure of the whole network. The layer 3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer 3 switches in the same autonomous system will have the same network topology map.

3） Each layer 3 switch uses the shortest path finding (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer 3 switch broadcast it so that additional information about the autonomous system can be recorded. As a result, the route table of each layer 3 switch is different.

OSPF protocol was developed by the IETF, and OSPF v2 widely used now is accordance to the content described in RFC2328.

18.4.2 OSPF Configuration

The OSPF configuration for DSCRS series switches may be different from the configuration procedure to switches of the other manufacturers. It is a two-step process:
1. Enable OSPF in the Global Mode;
2. Configure OSPF area for the interface.

18.4.2.1 Configuration Task Sequence

1. Enable OSPF (required)

(1) Enable/disable OSPF (required)

(2) Configure the ID number of the layer 3 switch running OSPF (optional)

(3) Configure the network scope for running OSPF (optional)

(4) Configure the area for the interface (required)

2. Configure OSPF sub-parameters (optional)

(1) Configure OSPF packet sending mechanism parameters

a. Configure OSPF packet verification

b. Set the OSPF interface to receive only

c. Configure the cost for sending packets from the interface

d. Configure OSPF packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer 3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

(2) Configure OSPF route introduction parameters

a. Configure default parameters (default type, default tag value, default cost, default interval and default number uplimit)

b. Configure the routes of the other protocols to introduce to OSPF.

(3) Configure other OSPF protocol parameters

a. Configure OSPF routing protocol priority

b. Configure cost for OSPF STUB area and default route

c. Configure OSPF virtual link

d. Configure the priority of the interface when electing designated layer 3 switch (DR).

3. Disable OSPF protocol.

1. Enable OSPF protocol

Basic configuration of OSPF routing protocol on ES4704BD series switches is quite simple, usually only enabling OSPF and configuration of the OSPF area for the interface are required. The OSPF protocol parameters can use the default settings. If OSPF protocol parameters need to be modified, please refer to "2. Configure OSPF sub-parameters".

Command	Explanation
Global Mode	
[no] router ospf	Enables OSPF protocol; the "**no router ospf**" command disables OSPF protocol (required)

router id <*router_id*> **no router id**	Configures the ID number for the layer 3 switch running OSPF; the "**no router id**" command cancels the ID number. The IP address of an interface is selected to be the layer 3 switch ID. (optional)
OSPF protocol configuration mode	
[no] network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]	Defines several segments in an area to a network scope; the "**no network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]**" command cancels the network scope. (optional)
Interface Mode	
ip ospf enable area <*area_id*> **no ip ospf enable area**	Sets an area for the specified interface; the "**no ip ospf enable area**" command cancels the setting. (required)

2. Configure OSPF sub-parameters

(1) Configure OSPF packet sending mechanism parameters

a. Configure OSPF packet verification

b. Set the OSPF interface to receive only

c. Configure the cost for sending packets from the interface

Command	Explanation
Interface Mode	
ip ospf authentication { simple <*auth_key*>| md5 <*auth_key*> <*key_id*>} **no ip ospf authentication**	Configures the authentication method and key required by the interface to accept OSPF packets; the "**no ip ospf authentication**" command restores the default setting.
[no] ip ospf passive-interface	Sets the interface to receive only, the "**no ip ospf passive-interface"** command cancels the setting.
ip ospf cost <*cost* > **no ip ospf cost**	Sets the cost for running OSPF on the interface; the "**no ip ospf cost**" command restores the default setting.

d. Configure OSPF packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer 3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.

Command	Explanation

Interface Mode	
ip ospf hello-interval <*time*> **no ip ospf hello-interval**	Sets interval for sending HELLO packets; the "**no ip ospf hello-interval**" command restores the default setting.
ip ospf dead-interval <*time* > **no ip ospf dead-interval**	Sets the interval before regarding a neighbor layer 3 switch invalid; the "**no ip ospf dead-interval**" command restores the default setting.
ip ospf transmit-delay <*time*> **no ip ospf transmit-delay**	Sets the delay time before sending link-state broadcast; the "**no ip ospf transmit-delay**" command restores the default setting.
ip ospf retransmit <*time*> **no ip ospf retransmit**	Sets the interval for retransmission of link-state advertisement among neighbor layer 3 switches; the "**no ip ospf retransmit**" command restores the default setting.

(2) Configure OSPF route introduction parameters

a. Configure default parameters (default type, default tag value, default cost, default interval and default number uplimit)

Command	Explanation
OSPF protocol configuration mode	
default redistribute type { 1 | 2 } **no default redistribute type**	Sets the default route weight for route to be introduced; the "**no default-metric**" command restores the default setting.
default redistribute tag <*tag*> **no default redistribute tag**	Sets the default tag value for introducing external routes; the "**no default redistribute tag**" command cancels the tag value setting.
default redistribute cost <*cost*> **no default redistribute cost**	Sets the default cost for introducing external routes; the "**no default redistribute cost**" command cancels the cost for introducing external routes. .
default redistribute interval <*time*> **no default redistribute interval**	Sets the interval for introducing external routes; the "**no default redistribute interval**" command restores the default setting.
default redistribute limit <*routes*> **no default redistribute limit**	Sets the maximum for external routes introduction; the "**no default redistribute limit**" command restores the default setting.

b. Configure the routes of the other protocols to introduce to OSPF.

Command	Explanation
OSPF protocol configuration mode	
redistribute ospfase { bgp | connected | static | rip} [type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>] ***no redistribute ospfase { bgp | connected | static | rip }***	Introduces BGP routes, direct routes, static routes and RIP routes as external routing information; the "**no redistribute ospfase { bgp | connected | static | rip }**" command cancels the introduction of external routing information.

(3) Configure other OSPF protocol parameters

a. Configure OSPF routing protocol priority

b. Configure cost for OSPF STUB area and default route

c. Configure OSPF virtual link

Command	Explanation
OSPF protocol configuration mode	
preference [ase] <*preference* > **no preference [ase]**	Configures the priority of OSPF among all the routing protocols, and the priority for AS exterior routes introduced; the "**no preference [ase]**" command restores the default setting.
stub cost <*cost*> area <*area_id* > **no stub area <area_id >**	Sets an area to STUB area; the "**no stub area <area_id >"** command cancels the setting.

virtuallink neighborid <*router_id*> transitarea <*area_id*> [hellointerval <*time*>] [deadinterval <*time*>] [retransmit <*time*>] [transitdelay <*time*>] **no virtuallink neighborid <*router_id*> transitarea <*area_id*>**	Creates and configures virtual link; the "**no virtuallink neighborid <*router_id*> transitarea <*area_id*>**" command deletes a virtual link.

d. Configure the priority of the interface when electing designated layer 3 switch (DR).

Command	Explanation
Interface Mode	
ip ospf priority <*priority*> **no ip ospf priority**	Sets the priority of the interface in "designated layer 3 switch" election; the "**no ip ospf priority**" command restores the default setting.

3. Disable OSPF protocol.

Command	Explanation
Global Mode	
no router ospf	Disables OSPF routing protocol

18.4.2.2 OSPF Configuration Commands

- **default redistribute cost**
- **default redistribute interval**
- **default redistribute limit**
- **default redistribute tag**
- **default redistribute type**
- **ip opsf authentication**
- **ip ospf cost**
- **ip opsf dead-interval**
- **ip ospf enable area**
- **ip ospf hello-interval**

- **ip ospf passive-interface**
- **ip ospf priority**
- **ip ospf retransmit-interval**
- **ip ospf transmit-delay**
- **network**
- **preference**
- **redistribute ospfase**
- **router id**
- **router ospf**
- **stub cost**
- **virtuallink neighborid**
- **show ip ospf**
- **show ip ospfase**
- **show ip ospf cumulative**
- **show ip ospf database**
- **show ip ospf interface**
- **show ip ospf neighbor**
- **show ip ospf routing**
- **show ip ospf virtual-links**
- **show ip protocols**
- **debug ip ospf event**
- **debug ip ospf lsa**
- **debug ip ospf packet**
- **debug ip ospf spf**

18.4.2.2.1 default redistribute cost

Command: default redistribute cost <*cost*>
no default redistribute cost

Function: Sets the default cost for introducing exterior routes into OSPF; the "**no default redistribute cost**" command restores the default setting.

Parameters: < *cost*> is the route cost, ranging from 1 to 65535.

Default: The default introducing cost is 1.

Command Mode: OSPF protocol configuration mode

Usage Guide: When OSPF routing protocol introduce the routes discovered by the other routing protocols, those routes are regarded as exterior autonomous system routing information. Introduction of exterior routing information requires some external parameter such as default cost and default tag for the routes. This command allows the user to set reasonable default cost for introducing exterior routes according to specific conditions

Example: Setting the default cost for OSPF to introduce exterior routes to 20.

Switch(Config-Router-Ospf)#default redistribute cost 20

18.4.2.2.2 default redistribute interval

Command: default redistribute interval <*time*>

no default redistribute interval

Function: Sets the interval for introducing external routes; the "**no default redistribute interval**" command restores the default setting.

Parameters: <***time***> is the interval for introducing exterior routes in seconds; the valid range is 1 to 65535 seconds.

Default: The default interval in OSPF for introducing exterior routes is 1 second.

Command Mode: OSPF protocol configuration mode

Usage Guide: OSPF introduces exterior routing information regularly and advertise the information throughout the autonomous system. This command is used to modify the interval for introducing exterior routing information.

Example: Setting the interval in OSPF for introducing exterior routes to 3 seconds.

Switch(Config-Router-Ospf)#default redistribute interval 3

18.4.2.2.3 default redistribute limit

Command: default redistribute limit <*routes*>

no default redistribute limit

Function: Sets the maximum exterior routes allowed in one route introduction; the "**no default redistribute limit**" command restores the default setting.

Parameters: < *value*> is the maximum number of routes allowed in one route introduction, ranging from 1 to 65535.

Default: The default exterior route allowed to be introduced in OSPF is 100.

Command Mode: OSPF protocol configuration mode

Usage Guide: OSPF introduces exterior routing information regularly and advertise the information throughout the autonomous system. This command mandates the maximum exterior routes allowed in one route introduction.

Example: Setting the maximum exterior routes allowed in one route introduction to 110.

Switch(Config-Router-Ospf)#default redistribute limit 110

18.4.2.2.4 default redistribute tag

Command: default redistribute tag <*tag*>

no default redistribute tag

Function: Sets the tag value for introducing exterior routes; the "**no default redistribute tag**" command restores the default setting.

Parameters: < *tag*> is the tag value, ranging from 0 to 4294967295.

Default: The default tag value is 0.

Command Mode: OSPF protocol configuration mode

Usage Guide: When OSPF routing protocol introduces routes discovered by the other routing protocols, those routes are regards as the exterior autonomous system routing information. Introduction of exterior routing information requires external parameters such as default cost and default tag for the routes. This command provides the user with information about tag identifying protocols.

Example: Setting the default tag value for OSPF to introduce exterior routes to 20000.

Switch(Config-Router-Ospf)#default redistribute tag 20000

18.4.2.2.5 default redistribute type

Command: default redistribute type { 1 | 2 }
no default redistribute type

Function: Sets the default route type(s) for exterior routes introduction; the "**no default redistribute type**" command restores the default setting.

Parameters: 1 and **2** stand for type1 and type2 exterior routes, respectively.

Default: The system assumes to introduce Type2 exterior routes by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: OSPF protocol divides exterior route information into 2 categories by cost selection method: type1 exterior route and type2 exterior route. The cost of type1 exterior route = advertised cost of exterior route + cost from a layer 3 switch to the advertising layer 3 switch (AS exterior layer 3 switch). Cost of type2 exterior route = advertised cost of exterior route. If both type1 and type2 exterior routes present, type1 routes take precedence.

Example: Setting the default exterior route type for OSPF to introduce to type1.

Switch(Config-Router-Ospf)#default redistribute type 1

18.4.2.2.6 ip ospf authentication

Command: ip ospf authentication { simple <*auth_key*>| md5 <*auth_key*> <*key_id*>}
no ip ospf authentication

Function: Configures the authentication method for the interface to accept OSPF packets; the "**no ip ospf authentication**" command cancels the authentication.

Parameters: simple stands for simple authentication; **md5** for MD5 encrypted authentication; **<*auth_key*>** for authentication key, which should be a string with no blank characters. Up to 8 bytes in simple authentication and 16 bytes in MD5 authentication are allowed; **<*key_id*>** is the checksum word for MD5 authentication, range from 1 to 255.

Default: Authentication is not required by default for the interface to accept OSPF packets.

Command mode: Interface Mode

Usage Guide: The value of key will be written into the OSPF packets to ensure proper OSPF packet sending/receiving between the layer 3 switch and neighbor layer 3 switches. The partner end must have the same "*key*" parameters set.

Example: Configuring MD5 authentication for OSPF interface vlan1 with an authentication password of "123abc".

Switch(Config-If-Vlan1)#ip ospf authentication md5 123abc 1

18.4.2.2.7 ip ospf cost

Command: ip ospf cost <*cost*>
no ip ospf cost

Function: Sets the cost for running OSPF on the interface; the "**no ip ospf cost**" command restores the default setting.

Parameters: < *cost*> is the OSPF cost, ranging from 1 to 65535.

Default: The default cost for OSPF protocol is 1.

Command mode: Interface Mode

Example: Setting the OSPF route cost of interface vlan1 to 3.
Switch(Config-If-Vlan1)#ip ospf cost 3

18.4.2.2.8 ip ospf dead-interval

Command: ip ospf dead-interval <*time* >
no ip ospf dead-interval
Function: Specifies the interval before regarding a neighbor layer 3 switch invalid; the "**no ip ospf dead-interval**" command restores the default setting.
Parameters: <***time***> is the timeout value for a neighbor layer 3 switch to be considered invalid in seconds; the valid range is 1 to 65535.
Default: The default timeout value for a neighbor layer 3 switch to be considered invalid is 40 seconds (usually 4 times of the hello-interval).
Command mode: Interface Mode
Usage Guide: If no HELLO packet is received from a neighbor layer 3 switch within the **dead-interval** time, that switch is considered unreachable and invalid. This command allows the user to set default time of a neighbor layer 3 switch to be considered invalid. The **dead-interval** value set will be written to the HELLO packet and send with it. For OSPF protocol to run properly, the **dead-interval** parameter between the interface and a neighbor layer 3 switch must be the same, and be at least four times of the **hello-interval** value.
Example: Setting the OSPF route invalid timeout value of interface vlan1 to 80 seconds..
Switch(Config-If-Vlan1)#ip ospf dead-interval 80

18.4.2.2.9 ospf enable area

Command: ip ospf enable area <*area_id*>
no ip ospf enable area
Function: Sets an area for the interface; the "**no ip ospf enable area**" command cancels the setting.
Parameters: **<*area_id*>** is the area number where the interface resides, ranging from 0 to 4294967295.
Default: The interface has no area configured by default.
Command mode: Interface Mode
Usage Guide: To run OSPF protocol on an interface, an area must be specified for that interface.
Example: Specifying interface vlan1 to area 1.
Switch(Config-If-Vlan1)#ip ospf enable area 1

18.4.2.2.10 ip ospf hello-interval

Command: ip ospf hello-interval <*time*>
no ip ospf hello-interval
Function: Configures the interval for sending HELLO packets from the interface; the "**no ip ospf hello-interval**" command restores the default setting.
Parameters: <***time***> is the interval for sending HELLO packets in seconds, ranging from 1 to 255.

Default: The default HELLO-packet-sending interval is 10 seconds.

Command mode: Interface Mode

Usage Guide: The HELLO packet is a most common packet sent to neighboring layer 3 switches regularly for discovering and maintaining the neighborhood and the election of DR and BDR. The **hello-interval** value set will be written to the HELLO packet and send with it. Smaller **hello-interval** enables faster discovery of network topology changes and incurs greater routing overhead. For OSPF protocol to run properly, the **hello-interval** parameter between the interface and the neighboring layer 3 switch must be the same.

Example: Setting the HELLO-packet-sending interval of interface vlan1 to 20 seconds.

Switch(Config-If-Vlan1)#ip ospf hello-interval 20

Related command: ip ospf dead-interval

18.4.2.2.11 ip ospf passive-interface

Command: ip ospf passive-interface

no ip ospf passive-interface

Function: Sets an interface to receive OSPF packets only, the "no **ip ospf passive-interface"** command cancels the setting.

Default: The interface receives/sends OSPF packets by default.

Command mode: Interface Mode

Example: Setting Ethernet interface vlan1 to receive OSPF packet only.

Switch(Config-If-Vlan1)#ip ospf passive-interface

18.4.2.2.12 ip ospf priority

Command: ip ospf priority <*priority*>

no ip ospf priority

Function: Set the priority of the interface in "designated layer 3 switch" (DR) election; the "**no ip ospf priority**" command restores the default setting.

Parameters: < *priority*> is the priority value, ranging from 0 to 255.

Default: The priority of the interface when electing designated layer 3 switch is 1.

Command mode: Interface Mode

Usage Guide: When two layer 3 switches in the same network segment want to be the "designated layer 3 switch" (DR), the DR is decided by the priority value, the switch with higher priority becomes the DR; if priority values are equal, the switch with the larger router-id is selected. When a layer 3 switch has a priority value of 0, it will not be elected to be either "designated layer 3 switch" or "backup designated layer 3 switch".

Example: Configuring the priority of the interface when electing a designated layer 3 switch (DR) and excluding interface vlan1 from the election, i.e., set the priority to 0.

Switch(Config-If-Vlan1)#ip ospf priority 0

18.4.2.2.13 ip ospf retransmit-interval

Command: ip ospf retransmit-interval <*time*>

no ip ospf retransmit-interval

Function: Sets the interval for retransmission of link-state advertisement among neighbor layer 3 switches; the "**no ip ospf retransmit**" command restores the default setting.

Parameters: <***time***> is the interval of link-state status advertisement retransmission to a neighbor layer 3 switch in seconds, ranging from 1 to 65535.

Default: The default retransmission interval is 5 seconds.

Command mode: Interface Mode

Usage Guide: When a layer 3 switch transfers link-state advertisement to its neighbor, it keeps advertising until an acknowledgement is received from the other end If no acknowledge packet is received within the interval set, it will resend the link-state advertisement. The retransmission interval must be greater than the time for a packet to travel to a layer 3 switch and return.

Example: Setting the re-authentication time of LSA for interface vlan1 to 10 seconds.

Switch(Config-If-Vlan1)#ip ospf retransmit 10

18.4.2.2.14 ip ospf transmit-delay

Command: ip ospf tranmsit-delay <*time*>

no ip ospf transmit-delay

Function: Sets the delay time before sending link-state advertisement (LSA); the "**no ip ospf transmit-delay**" command restores the default setting.

Parameters: **<*time*>** is the delay time for the link-state advertisement transmission in seconds, ranging from 1 to 65535.

Default: The default LSA sending interval is 1 second.

Command mode: Interface Mode

Usage Guide: LSA aging occurs on the local layer 3 switch but not during network transmission, therefore, adding a delay of **transmit-delay** allows the LSA to be sent before it is aged.

Example: Setting the delay time for interface vlan1 to send LSA to 2 seconds.

Switch(Config-If-Vlan1)#ip ospf transmit-delay 2

18.4.2.2.15 network

Command: network <*network*> <*mask*> area <*area_id*> [advertise | notadvertise]

no network <*network*> <*mask*> area <*area_id*>

Function: Specifies the area of each network in the layer 3 switch; the "**no network <*network*> <*mask*> area <*area_id*>"** command deletes the setting.

Parameters: **<*network*>** and **<*mask*>** are the network IP address and mask in decimal format; **<*area_id*>** is the area number from 0 to 4294967295; **advertise | notadvertise** specifies whether or not broadcast the summary route information within the network.

Default: The system has no default area configured; if configured, it assumes to broadcast summary information by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: Once a part of a network joins an area, all interior routes of that network will no longer be broadcasted to the other areas independently, but the summary information for that whole network.. The introduction of network scope and scope limit can reduce routing information traffic between areas.

Example: Specifying network scope 10.1.1.0, 255.255.255.0 to join area 1.

Switch(Config-Router-Ospf)#network 10.1.1.0 255.255.255.0 area 1

18.4.2.2.16 preference

Command: preference [ase] <*preference* >

no preference [ase]

Function: Configures the priority of OSPF among all the routing protocols, and the priority for AS exterior routes introduced; the "**no preference [ase]**" command restores the default setting.

Parameters: ase means the priority is used when introducing exterior routes outside the AS; **<*preference* >** is the priority value ranging from 1 to 255.

Default: The default priority of OSPF protocol is 110; the default priority to introduce exterior route is 150.

Command Mode: OSPF protocol configuration mode

Usage Guide: As a layer 3 switch may have several dynamic routing protocol running, there arises the issue of information sharing and selection among routing protocols. For this reason, each routing protocol has a default priority,. When the same route is discovered by different protocols, the one with the higher priority overrules. Priority changes will be applied on newly constructed routes. Due to the nature of OSPF, the OSPF priority should not be set too low.

Example: Setting in OSPF the default priority to introduce ASE route to 20.

Switch(Config- Router-Ospf)#preference ase 20

18.4.2.2.17 redistribute ospfase

Command: redistribute ospfase { bgp |connected | static | rip} [type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>]

no redistribute ospfase { bgp |connected | static | rip}

Function: Introduces BGP routes, direct routes, static routes and RIP routes as external routing information; the "no redistribute ospfase { bgp | connected | static | rip }" command cancels the introduction of external routing information.

Parameters: bgp stands for introduce BGP routes as the exterior route information source; **connected** for direct routes; **static** for static routes; **rip** for routes discovered by RIP; **type** specifies the type of exterior routes, **1** and **2** represent type1 exterior routes and type2 exterior routes, respectively; **tag** specifies the tag of the routes, **<*tag*>** is the tag value for the routes, ranging from 0 to 4,294,967,295; **metric** specifies the weight of the route; **<*cost_value*>** for weight value, ranging from 1 to 16,777,215.

Default: Exterior routes are not introduced in OSPF by default.

Command Mode: OSPF protocol configuration mode

Usage Guide: Routing information can be shared among all dynamic routing protocols in layer 3 switches. Due to the nature of OSPF, the routes discovered by the other routing protocols are regards as the exterior autonomous system routing information.

Example: introducing RIP routes as type1 exterior routes in OSPF, with a tag value of 3 and an introducing cost of 20.

Switch(Config-Router-Ospf)#redistribute ospfase rip type 1 tag 3 metric 20

18.4.2.2.18 router id

Command: router id <*router_id*>

no router id

Function: Configures the ID number for the layer 3 switch running OSPF; the "**no router id**" command cancels the ID number.

Parameters: <*router_id*> is the ID number for the layer 3 switch in decimal format.

Default: No layer 3 switch ID number is configured by default, an address from the IP addresses of all the interfaces is selected to be the layer 3 switch ID number.

Command mode: Global Mode

Usage Guide: OSPF use a layer 3 switch ID number as a unique identity for the layer 3 switch in an autonomous system, usually the address of an interface running OSPF. ES4704BD layer 3 switch uses the first IP layer 3 interface in the switch as the router id by default. If no IP address is configured in all interfaces of the layer 3 switch, this command must be used to specify the layer 3 switch ID number, otherwise OSPF will not work. Changes to a layer 3 switch ID number will apply only after the restart of OSPF.

Example: Configuring the ID of the layer 3 switch to 10.1.120.1.

Switch(Config)#router id 10.1.120.1

18.4.2.2.19 router ospf

Command: router ospf

no router ospf

Function: Enables OSPF protocol and enters OSPF mode after enabling; the "**no router ospf**" command disables OSPF protocol.

Default: OSPF is disabled by default.

Command mode: Global Mode

Usage Guide: Use this command to enable or disable OSPF protocol. Configurations to OSPF will only take effect when OSPF is enabled.

Example: Enabling OSPF on the switch.

Switch(Config)#router ospf

18.4.2.2.20 stub cost

Command: stub cost <*cost*> area <*area_id* >

no stub area <*area_id* >

Function: Sets an area to STUB area; the "**no stub area <area_id >"** command cancels the setting.
Parameters: <***cost***> is the default route cost for the STUB area, ranging from 1 to 65535; <***area_id***> is the area number of the STUM area, ranging from 1 to 4,294,967,295.
Default: No STUB area is configured by default.
Command Mode: OSPF protocol configuration mode
Usage Guide: An area can be configured to a STUB area if the area has only one egress point (connect to one layer 3 switch only), or need not select egress point for each exterior destination. Type4 LSA (ASBR summary LSA) and type5 LSA (AS exterior LSA) are not allowed to flood into/through STUB areas, this saves the resource for processing exterior routing information for layer 3 switches inside the area.
Example: Setting area 1 to be a STUB area with a default routing cost of 60.
Switch(Config-Router-Ospf)#stub cost 60 area 1

18.4.2.2.21 virtuallink neighborid

Command: virtuallink neighborid <*router_id*> transitarea <*area_id*> [hellointerval <*time*>] [deadinterval <*time*>] [retransmit<*time*>] [transitdelay <*time*>]
no virtuallink neighborid <*router_id*> transitarea <*area_id*>
Function: Creates and configures a virtual link; the "**no virtuallink neighborid <*router_id*> transitarea <*area_id*>**" command deletes a virtual link.
Parameters: <***router_id***> is the ID for the virtual link neighbor in decimal format; <***area_id***> is the area number for transit area, ranging from 0 to 42,949,67,295; the last four parameters are optional intervals that have the same meaning as those in OSPF interface mode.
Default: No virtual link is configured by default.
Command Mode: OSPF protocol configuration mode
Usage Guide: The introduction of virtual link is to fulfill or enhance the connectivity of the backbone area (area 0). As the backbone area must be kept connected logically, if no in-area route exists between two nodes within the backbone area, a virtual link must be established between the two nodes across a transit area. Virtual links are identified by the ID of the partner layer 3 swtich. The non-backbone area providing interior route for both ends of the virtual link is referred to a "transit area", the area number must be specified on configuration.
A virtual link is activated when the route across the transit area is calculated, and practically forms a point-to-point connection between the two ends. In this connection, interface parameters (such as HELLO interval) can be configured just as on a physical interface.
Example: Configuring a virtual link to 11.1.1.1 via transit area 2.
Switch(Config-Router-Ospf)#virtuallink neighborid 11.1.1.1 transitarea 2

18.4.2.2.22 show ip ospf

Command: show ip ospf
Function: Displays major OSPF information.
Default: Nothing displayed by default
Command mode: Admin Mode

Example:

```
Switch#show ip ospf
my router ID is 11.11.4.1
preference=10      ase perference=150
export metric=1
export tag=-2147483648
area ID    0
     interface count：1
     80times spf has been run for this area
     net range：
LSRefreshTime is1800
area ID    1
     interface count：1
     41times spf has been run for this area
     net range：
netid11.11.3.255      netaddress11.11.0.0      netmask255.255.252.0
LSRefreshTime is1800
```

Displayed information	Explanation
my router ID	The ID of the current layer 3 switch.
Preference	Routing protocol priority.
ase perference	Exterior routes priority for introduction.
export metric	The metrics for output from the port
export tag	The route tag for output from the port.
area ID interface count imes spf has been run for this area net range	OSPF area number: including statistics for interface number in the area, SPF algorithm calculation time and network scope.

18.4.2.2.23 show ip ospf ase

Command: show ip ospf ase

Function: Displays exterior OSPF routing information.

Default: Nothing displayed by default

Command mode: Admin Mode

Example:

```
Switch#show ip ospf ase
Destination     AdvRouter    NextHop    Age    SeqNumber      Type    Cost
10.1.1.125      11.11.1.2    11.1.1.2   3      300            2       20
```

Displayed information	Explanation

Destination	Target network segment or address
AdvRouter	Route election
NextHop	Next hop address
Age	Aging time
SeqNumber	Sequence number
Type	Exterior routes type for introduction
Cost	Cost for introducing exterior routes

18.4.2.2.24 show ip ospf cumulative

Command: show ip ospf cumulative

Function: Displays OSPF statistics.

Default: Nothing displayed by default

Command mode: Admin Mode

Example:

Switch#show ip ospf cumulative

IO cumulative

type in out

HELLO 1048 253

DD 338 337

LS Req 62 219

LS Update 753 295

LS Ack 495 308

ASE count 0 checksum 0

original LSA 340 LS_RTR 179 LS_NET 1 LS_SUM_NET 160 LS_SUM_ASB 0 LS_ASE 0

received LSA 325

Areaid 0

nbr count 1 interface count 1

spf times 120

DB entry count 6

LS_RTR 2 LS_NET 2 LS_SUM_NET 3 LS_SUM_ASB 0 LS_ASE 3

Areaid 1

nbr count 2 interface count 1

spf times 52

DB entry count 6

LS_RTR 3 LS_NET 3 LS_SUM_NET 1 LS_SUM_ASB 0 LS_ASE 3

AS internal route 4 AS external route 0

Displayed information	Explanation

IO cumulative	Statistics for OSPF packets in/out.
Type	Packet type: including HELLO packet, DD packet, LS request, update and acknowledging packet, etc.
In	Packet in statistics.
Out	Packet out statistics.
Areaid	OSPF statistics from a specific OSPF area.

18.4.2.2.25 show ip ospf database

Command: show ip ospf database [{asb-summary| external | network | router | summary}]

Function: Display OSPF link-state database information.

Default: Nothing displayed by default

Command mode: Admin Mode

Usage Guide: OSPF link-state database information can be checked by the output of this command.

Example:

Switch#show ip ospf database

OSPF router ID：11.11.4.1 AS：No

Area 1>>>>>>>> Area ID： 0

Router LSAs

LS ID (Router ID)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Router LSA

11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Network LSAs

LS ID (DR's IP)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.4.2	11.11.4.2	1	2147483662	1	35126

Summary Network LSAs

LS ID (Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.1.0	11.11.4.1	0	2147483656	1	6777215
11.11.2.255	11.11.4.1	0	2147483649	1	6777215
11.11.3.255	11.11.4.1	0	2147483680	1	6777215

ASBR Summary LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(ASBR's Rtr ID)

Area 2>>>>>>>> Area ID： 1

Router LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(Router ID)
11.11.2.1 11.11.2.1 1 2147483698 1 6777215
14.14.14.1 14.14.14.1 1 2147483662 1 14831
11.11.4.1 11.11.4.1 0 2147483669 0 33875
Router LSA
11.11.2.1 11.11.2.1 1 2147483698 1 6777215

14.14.14.1 14.14.14.1 1 2147483662 1 14831

11.11.4.1 11.11.4.1 0 2147483669 0 33875

Network LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(DR's IP)
11.11.1.1 11.11.4.1 0 2147483649 1 6777215
11.11.1.3 14.14.14.1 15 2147483705 1 53384

Summary Network LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(Net's IP)
11.11.4.255 11.11.4.1 0 2147483677 1 6777215

ASBR Summary LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(ASBR's Rtr ID)

AS External LSAs

LS ID Route type ADV rtr Age Sequence Cost Checksu Forw addr RouteTag
(Ext Net's IP)

Displayed information	Explanation
OSPF router ID	The ID of the layer 3 switch.
Area 1>>>>>>>> Area ID： 0	Represent the LSA database information from area 1 to area 0.
Router LSAs	Route LSA

Network LSAs	Network LSA
Summary Network LSAs	Summary network LSA
ASBR Summary LSAs	Autonomous system exterior LSA

18.4.2.2.26 show ip ospf interface

Command: show ip ospf interface <*interface*>

Function: Displays OSPF interface information.

Parameters: <*interface*> stands for the interface name.

Default: Nothing displayed by default

Command mode: Admin Mode

Example:

Switch#show ip ospf interface vlan 1

IP address： 11.11.4.1 Mask： 255.255.255.0 Area： 0

Net type： BROADCAST cost： 1

State： IBACKUP Type： BDR

Priority： 1 Transit Delay： 1

DR： 11.11.4.2 BDR： 11.11.4.1

Authentication key：

Timer： Hello：10 Poll： 0 Dead： 40 Retrans： 5

Number of Neigbors： 1 Nubmer of Adjacencies： 1

Adjacencies：

1： 11.11.4.2

Displayed information	Explanation
IP address	Interface IP address
Mask	Interface mask.
Area	The area of the interface
Net type	Network type, such as broadcast, p2mp, etc.
Cost	Cost value
State	Status
Type	Layer 3 switch type, such as designated
Priority	Configures the priority in electing designated layer 3 switch.
Transit Delay	The delay value for interface to transfer LAS.
DR	The designated layer 3 switch.
BDR	Backup designated layer 3 switch.
Authentication key	OSPF packet authentication key
Timer Hell, Poll, Dea, Retrans	OSPF protocol timer: including time set for HELLO packet, Poll interval packet, route invalid, route retransmission, etc.
Number of Neigbors	The number of neighboring layer 3 switches

Nubmer of Adjacencies	The number of neighboring route interfaces
Adjacencies	Neighboring interface IP address

18.4.2.2.27 show ip ospf neighbor

Command: show ip ospf neighbor

Function: Displays OSPF neighbor node information

Default: Nothing displayed by default

Command mode: Admin Mode

Usage Guide: OSPF neighbor information can be checked by the output of this command.

Example:

```
Switch#show ip ospf neighbor
interface ip 12.1.1.1        area id 0
   router id 12.1.1.2         router ip addr 12.1.1.2
   state NFULL        priority 1
   DR 12.1.1.2          BDR 12.1.1.1
   last hello 59006        last exch 49717
interface ip 30.1.1.1        area id 0
interface ip 50.1.1.1        area id 0
   router id 50.1.1.2         router ip addr 50.1.1.2
   state NFULL        priority 0
   DR 50.1.1.1          BDR 0.0.0.0
   last hello 59010        last exch 49614
interface ip 51.1.1.1        area id 0
interface ip 52.1.1.1        area id 0
interface ip 100.1.1.1        area id 0
interface ip 110.1.1.1        area id 0
interface ip 150.1.1.1        area id 0
   router id 12.2.0.0         router ip addr 150.1.1.2
   state NFULL        priority 0
   DR 150.1.1.1          BDR 0.0.0.0
   last hello 59011        last exch 49607
```

Displayed information	Explanation
interface ip	IP address of an interface in the current layer 3 switch
area id	ID of the area for the interface
router id	ID of the neighbor layer 3 switch
router ip addr	IP address of the interface in the neighboring layer 3 switch
State	Link-state status
Priority	Priority

DR	ID of the designated layer 3 switch
BDR	ID of the backup designated layer 3 switch
last hello	The last HELLO packet
last exch	The last packet exchanged

18.4.2.2.28 show ip ospf routing

Command: show ip ospf routing

Function: Displays OSPF route table information.

Default: Nothing displayed by default

Command mode: Admin Mode

Example:

Switch#show ip ospf routing

AS internal routes：

Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
60.2.127.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.1.132.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.4.67.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.3.72.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2
60.2.77.0	0	7	DTYPE_NET	12.1.1.2	6.1.1.2

AS external routes：

Destination	Cost	Dest Type	Next Hop	ADV rtr

Displayed information	Explanation
AS internal routes	Autonomous system interior route
AS external routes	Autonomous system exterior route
Destination	Destination network segment
Area	Area number
Cost	Cost value
Dest Type	Route Type
Next Hop	Next hop
ADV rtr	Advertise the interface address of the layer 3 switch

18.4.2.2.29 show ip ospf virtual-links

Command: show ip ospf virtual-links

Function: Displays OSPF virtual link information.

Default: Nothing displayed by default

Command mode: Admin Mode

Example:

Switch#show ip ospf virtual-links
no virtual-link

18.4.2.2.30 show ip protocols

Command: show ip protocols
Function: Displays the information of the routing protocols running in the switch.
Command mode: Admin Mode
Usage Guide: The user can decide whether the routing protocols configured are correct and perform routing troubleshooting according to the output of this command.
Example:
Switch#sh ip protocols
OSPF is running.
my router ID is 100.1.1.1
preference=10 ase perference=150
export metric=1
export tag=-2147483648
area ID 1
interface count:2
7times spf has been run for this area
net range:
LSRefreshTime is1800
RIP information
rip is shutting down

Displayed information	Explanation
OSPF is running	The running routing protocol is OSPF protocol.
My router ID	The ID number of the layer 3 switch running
Preference	OSPF routing priority
Ase perference	Autonomous system exterior routes priority
Export metric	Metrics for exporting OSPF routes
Export tag	Tag value for exporting OSPF routes
Area ID	The ID of the OSPF area where the current layer 3 switch resides
Interface count	Number of interfaces running OSPF routing protocol
N times spf has been run for this area	Number of times the layer 3 switch performs minimum tree spanning calculation
Net range	The network scope for running OSPF protocol
LSRefreshTime	Link-state advertisement (LSA) update interval of OSPF protocol

18.4.2.2.31 debug ip ospf event

Command: debug ip ospf event

no debug ip ospf event

Function: Enables the OSPF debugging function for all events: the "**no debug ip ospf event**" command disables the debug function.

Default: Debugging is disabled by default.

Command mode: Admin Mode

18.4.2.2.32 debug ip ospf lsa

Command: debug ip ospf lsa

no debug ip ospf lsa

Function: Enables the link-state status advertisement debug function: the "**no debug ip ospf lsa**" command disables the debug function.

Default: Debugging is disabled by default.

Command mode: Admin Mode

18.4.2.2.33 debug ip ospf packet

Command: debug ip ospf packet

no debug ip ospf packet

Function: Enables the OSPF packet debug function; the "**no debug ip ospf packet**" command disables this debug function.

Default: Debugging is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug ip ospf packet

packet length： 44

02：40：54：

receive ACK from 11.11.1.3

02：40：56：

receive a packet from 11.11.1.2

packet length： 44

02：40：56：

receive ACK from 11.11.1.2

02：40：58：

receive a packet from 11.11.4.2

packet length： 48

02：40：58：

receive a HELLO packet from 11.11.4.2 via Broadcast interface 11.11.4.1

02：40：58：

18.4.2.2.34 debug ip ospf spf

Command: debug ip ospf spf

no debug ip ospf spf

Function: Enables the OSPF debug function for shortest path algorithm; the "**no debug ip ospf spf**" command disables this debug function.

Default: Debugging is disabled by default.

Command mode: Admin Mode

18.4.3 Typical OSPF Scenario

Scenario 1: OSPF autonomous system.

This scenario takes an OSPF autonomous system consists of five ES4704BD layer 3 switches for example, where layer 3 switch Switch1 and Switch5 make up OSPF area 0, layer 3 switch Switch2 and Switch3 form OSPF area 1 (assume vlan1 interface of layer 3 switch Switch1 belongs to area 0), layer 3 switch Switch4 forms OSPF area2 (assume vlan2 interface of layer 3 Switch5 belongs to area 0). Swtich1 and Switch5 are backbone layer 3 switches, Swtich2 and Switch4 are area edge layer 3 switches, and Switch3 is the in-area layer 3 switch.

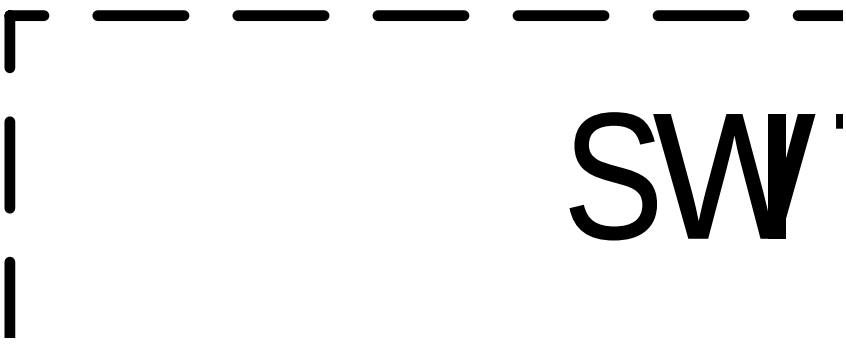


Fig 18-3 Network topology of OSPF autonomous system.

The configuration for layer 3 switch Switch1 and Switch5 is shown below:

Layer 3 switch Switch1:

!Configuration of the IP address for interface vlan1

Switch1#config

Switch1(Config)# interface vlan 1

Switch1(Config-if-vlan1)# ip address 10.1.1.1 255.255.255.0

Switch1(Config-if-vlan1)#no shut-down

Switch1(Config-if-vlan1)#exit

! Configuration of the IP address for interface vlan2

Switch1(Config)# interface vlan 2

```
Switch1(Config-if-vlan2)# ip address 100.1.1.1 255.255.255.0
Switch1 (Config-if-vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan1 and vlan2.
Switch1(Config)#router ospf
Switch1(Config-router-ospf)#exit
Switch1(Config)#interface vlan 1
Switch1 (Config-if-vlan1)#ip ospf enable area 0
Switch1 (Config-if-vlan1)#exit
Switch1(Config)#interface vlan2
Switch1 (Config-if-vlan2)#ip ospf enable area 0
Switch1 (Config-if-vlan2)#exit
Switch1(Config)#exit
Switch1#
```

Layer 3 switch Switch2:

```
!Configure the IP address for interface vlan1 and vlan2.
Switch2#config
Switch2(Config)# interface vlan 1
Switch2(Config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
Switch2(Config-if-vlan1)#no shut-down
Switch2(Config-if-vlan1)#exit
Switch2(Config)# interface vlan 3
Switch2(Config-if-vlan3)# ip address 20.1.1.1 255.255.255.0
Switch2(Config-if-vlan3)#no shut-down
Switch2(Config-if-vlan3)#exit
！Enable OSPF protocol, configure the OSPF area interfaces vlan1 and vlan3 in.
Switch2(Config)#router ospf
Switch2(Config-router-ospf)#exit
Switch2(Config)#interface vlan 1
Switch2(Config-if-vlan1)#ip ospf enable area 0
Switch2(Config-if-vlan1)#exit
Switch2(Config)#interface vlan 3
Switch2(Config-if-vlan3)#ip ospf enable area 1
Switch2(Config-if-vlan3)#exit
Switch2(Config)#exit
Switch2#
```

Layer 3 switch Switch3:

```
!Configuration of the IP address for interface vlan3
Switch3#config
Switch3(Config)# interface vlan 3
```

Switch3(Config-if-vlan1)# ip address 20.1.1.2 255.255.255.0

Switch3(Config-if-vlan3)#no shut-down

Switch3(Config-if-vlan3)#exit

！Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in.

Switch3(Config)#router ospf

Switch3(Config-router-ospf)#exit

Switch3(Config)#interface vlan 3

Switch3(Config-if-vlan3)#ip ospf enable area 1

Switch3(Config-if-vlan3)#exit

Switch3(Config)#exit

Switch3#

Layer 3 switch Switch4:

!Configuration of the IP address for interface vlan3

Switch4#config

Switch4(Config)# interface vlan 3

Switch4(Config-if-vlan3)# ip address30.1.1.2 255.255.255.0

Switch4(Config-if-vlan3)#no shut-down

Switch4(Config-if-vlan3)#exit

！Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in.

Switch4(Config)#router ospf

Switch4(Config-router-ospf)#exit

Switch4(Config)#interface vlan 3

Switch4(Config-if-vlan3)#ip ospf enable area 0

Switch4(Config-if-vlan3)#exit

Switch4(Config)#exit

Switch4#

Layer 3 switch Switch5:

!Configuration of the IP address for interface vlan2

Switch5#config

Switch5(Config)# interface vlan 2

Switch5(Config-if-vlan2)# ip address 30.1.1.1 255.255.255.0

Switch5(Config-if-vlan2)#no shut-down

Switch5(Config-if-vlan2)#exit

! Configuration of the IP address for interface vlan3

Switch5(Config)# interface vlan 3

Switch5(Config-if-vlan3)# ip address 100.1.1.2 255.255.255.0

Switch5(Config-if-vlan3)#no shut-down

Switch5(Config-if-vlan3)#exit

！Enable OSPF protocol, configure the number of the area in which interface vlan2 and vlan3

reside in.

```
Switch5(Config)#router ospf
Switch5(Config-router-ospf)#exit
Switch5(Config)#interface vlan 2
Switch5(Config-if-vlan2)#ip ospf enable area 0
Switch5(Config-if-vlan2)#exit
Switch5(Config)#interface vlan 3
Switch5(Config-if-vlan3)#ip ospf enable area 0
Switch5(Config-if-vlan3)#exit
Switch5(Config)#exit
Switch5#
```

Scenario 2: Typical OSPF protocol complex topology.

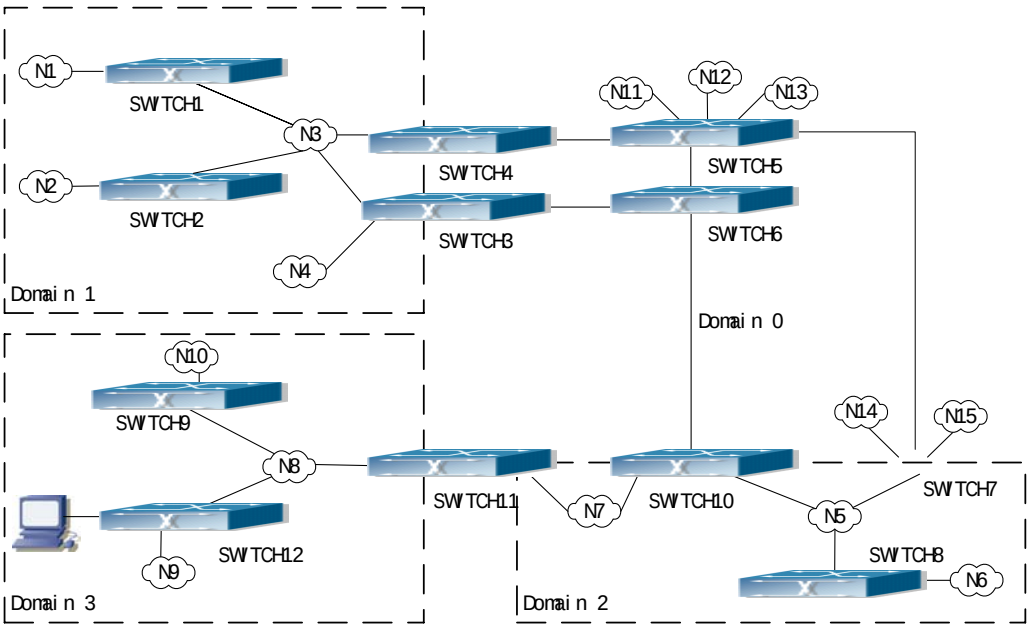


Fig 18-4 Typical complex OSPF autonomous system.

Figure 18-4 is a typical complex OSPF autonomous system network topology. Area1 include network N1-N4 and layer 3 switch Switch1-Switch4, area2 include network N5-N7 and layer 3 switch Switch7, Switch8, Switch10 and Switch11, area3 include N8-N10, host H1 and layer 3 switch Switch9, Switch11 and Switch12, and network N8-N10 share a same summary route with host H1(i.e., define area3 and a STUB area). Layer 3 switch Switch1, Switch2, Switch5, Switch6, Switch8, Switch9, Switch12 are in-area layer 3 switches, Switch3, Switch4, Switch7, Switch10 and Switch11 are edge layer 3 switches of the area, Switch5 and Switch7 are edge layer 3 switches of the autonomous system.

To area1, layer 3 switches Switch1 and Switch2 are both in-area switches, area edge switches Switch3 and Switch4 are responsible for reporting distance cost to all destination outside the area, while they are also responsible for reporting the position of the AS edge layer 3 switches Switch5 and Switch7, AS exterior link-state advertisement from Switch5 and Switch7 are flooded throughout the whole autonomous system. When ASE LSA floods in area 1, those LSA are included in the area 1 database to get the routes to network N11 and N15.

In addition, layer 3 switches, Switch3 and Switch4, must summary the topology of area 1 to the backbone area (area 0, all non-0 areas must be connected via area 0, direct connections are not allowed), and advertise the networks in area 1 (N1-N4) and the costs from Switch3 and Switch4 to those networks. As the backbone area is required to maintain connection, there must be a virtual link between backbone layer 3 switch Switch10 and Switch11. The area edge layer 3 switches exchange summary information via the backbone layer 3 switch, each area edge layer 3 switch listens to the summary information from the other edge layer 3 switches.

Virtual links can not only maintain the connectivity of the backbone area, but also strengthen the backbone area. For example, if the connection between backbone layer 3 switch Switch8 and Switch10 is cut down, the backbone area will become discontinued. The backbone area can become more robust by establishing a virtual link between backbone layer 3 switches Switch7 and Switch10. In addition, the virtual link between Switch7 and Switch10 provides a short path from area 3 to layer 3 switch Switch7.

Take area 1 as an example. Assume the IP address of layer 3 switch Switch1 is 10.1.1.1, IP address of layer 3 switch Switch2 interface VLAN2 is 10.1.1.2, IP address of layer 3 switch Switch3 interface VLAN2 is 10.1.1.3, IP address of layer 3 switch Switch4 interface VLAN2 is 10.1.1.4. Switch1 is connecting to network N1 through Ethernet interface VLAN1 (IP address 20.1.1.1); Switch2 is connecting to network N2 through Ethernet interface VLAN1 (IP address 20.1.2.1); Switch3 is connecting to network N4 through Ethernet interface VLAN3 (IP address 20.1.3.1). All the three addresses belong to area 1. Switch3 is connecting to layer 3 switch Switch6 through Ethernet interface VLAN1 (IP address 10.1.5.1); Switch4 is connecting to layer 3 switch Switch5 through Ethernet interface VLAN1 (IP address 10.1.6.1); both two addresses belong to area 1. Simple authentication is implemented among layer 3 switches in area1, edge layer 3 switches of area 1 authenticate with the area 0 backbone layer 3 switches by MD5 authentication.

The followings are just configurations for layer 3 switches in area 1, configurations for layer 3 switches of the other areas are omitted. The following are the configurations of Switch1 Switch2.Switch3 and Switch4:

1)Switch1：

```
!Configuration of the IP address for interface vlan2
Switch1#config
Switch1(Config)# interface vlan 2
Switch1(Config-If-Vlan2)# ip address 10.1.1.1 255.255.255.0
Switch1(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch1(Config)#router ospf
```

```
Switch1(Config-router-ospf)#exit
Switch1(Config)#interface vlan 2
Switch1(Config-If-Vlan2)#ip ospf enable area 1

!Configure simple key authentication.
Switch1(Config-If-Vlan2)#ip ospf authentication simple Edge-core
Switch1(Config-If-Vlan2)exit
!Configuration of the IP address and area number for interface vlan1
Switch1(Config)# interface vlan 1
Switch1(Config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
Switch1(Config-If-Vlan1)#ip ospf enable area 1
Switch1(Config-If-Vlan1)#exit
```

2)Switch2：

```
!Configuration of the IP address for interface vlan2
Switch2#config
Switch2(Config)# interface vlan 2
Switch2(Config-If-Vlan2)# ip address 10.1.1.2 255.255.255.0
Switch2(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch2(Config)#router ospf
Switch2(Config-router-ospf)#exit
Switch2(Config)#interface vlan 2
Switch2(Config-If-Vlan2)#ip ospf enable area 1
!Configure simple key authentication.
Switch2(Config-If-Vlan2)#ip ospf authentication simple Edge-core
Switch2(Config-If-Vlan2)#exit
!Configuration of the IP address and area number for interface vlan1
Switch2(Config)# interface vlan 1
Switch2(Config-If-Vlan1)#ip address 20.1.2.1 255.255.255.0
Switch2(Config-If-Vlan1)#ip ospf enable area 1
Switch2(Config-If-Vlan1)#exit
Switch2(Config)#exit
Switch2#
```

3)Switch3：

```
!Configuration of the IP address for interface vlan2
Switch3#config
Switch3(Config)# interface vlan 2
Switch3(Config-If-Vlan2)# ip address 10.1.1.3 255.255.255.0
Switch3(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch3(Config)#router ospf
```

Switch3(Config-router-ospf)#exit
Switch3(Config)#interface vlan 2
Switch3(Config-If-Vlan2)#ip ospf enable area 1
!Configure simple key authentication.
Switch3(Config-If-Vlan2)#ip ospf authentication simple Edge-core
Switch3(Config-If-Vlan2)#exit
!Configuration of the IP address and area number for interface vlan3
Switch3(Config)# interface vlan 3
Switch3(Config-If-Vlan3)#ip address 20.1.3.1 255.255.255.0
Switch3(Config-If-Vlan3)#ip ospf enable area 1
Switch3(Config-If-Vlan3)#exit
!Configuration of the IP address and area number for interface vlan1
Switch3(Config)# interface vlan 1
Switch3(Config-If-Vlan1)#ip address 10.1.5.1 255.255.255.0
Switch3(Config-If-Vlan1)#ip ospf enable area 0
!Configure MD5 key authentication.
Switch3 (Config-If-Vlan1)#ip ospf authentication md5 Edge-core
Switch3 (Config-If-Vlan1)#exit
Switch3(Config)#exit
Switch3#
4)Switch4：
!Configuration of the IP address for interface vlan2
Switch4#config
Switch4(Config)# interface vlan 2
Switch4(Config-If-Vlan2)# ip address 10.1.1.4 255.255.255.0
Switch4(Config-If-Vlan2)#exit
！Enable OSPF protocol, configure the area number for interface vlan2.
Switch4(Config)#router ospf
Switch4(Config-router-ospf)#exit
Switch4(Config)#interface vlan 2
Switch4(Config-If-Vlan2)#ip ospf enable area 1
!Configure simple key authentication.
Switch4(Config-If-Vlan2)#ip ospf authentication simple Edge-core
Switch4(Config-If-Vlan2)#exit
!Configuration of the IP address and area number for interface vlan1
Switch4(Config)# interface vlan 1
Switch4(Config-If-Vlan1)# ip address 10.1.6.1 255.255.255.0
Switch4(Config-If-Vlan1)#ip ospf enable area 0

!Configure MD5 key authentication.

Switch4(Config-If-Vlan1)#ip ospf authentication md5 Edge-core

Switch4(Config-If-Vlan1)exit

Switch4(Config)#exit
Switch4#

18.4.4 OSPF Troubleshooting Help

1. Monitor and Debugging Commands
2. OSPF Troubleshooting Help

18.4.4.1 Monitor and Debugging Commands

Command	Explanation
Admin Mode	
Show interface	Displays interface information to verify the interface and datalink layer protocols are up.
Show ip ospf	Displays the current running status and configuration information for OSPF. Users can decide if configurations are correct and perform OSPF troubleshooting according to the output.
Show ip route	Displays route table information, OSPF routing information can be checked.
Show ip ospf ase	Displays exterior OSPF routing information
Show ip ospf cumulative	Displays OSPF statistics
Show ip ospf database	Displays OSPF link-state database information
Show ip ospf interface	Displays OSPF information for the specified interface
Show ip ospf neighbor	Displays OSPF neighbor information
Show ip ospf routing	Displays OSPF route table information
Show ip ospf virtual-links	Displays OSPF virtual link information
Show ip protocols	Displays information for running routing protocols
[no] debug ip ospf event	Displays all event information for OSPF debug; the "**no debug ip ospf event**" command disables this debug function
[no] debug ip ospf lsa	Displays information for link-state advertisements; the "**no debug ip ospf lsa**" command disables this debug function
[no] debug ip ospf packet	Displays information for OSPF packets; the "**no debug ip ospf packet**" command disables this debug function
[no] debug ip ospf spf	Displays SPF information for debug; the "**no debug ip ospf spf**" command disables the debugging function.

（1）show ip ospf

Example:

Switch#show ip ospf
my router ID is 11.11.4.1
preference=10 ase perference=150
export metric=1
export tag=-2147483648
area ID 0
interface count：1
80times spf has been run for this area
net range：
LSRefreshTime is1800
area ID 1
interface count：1
41times spf has been run for this area
net range：
netid11.11.3.255 netaddress11.11.0.0 netmask255.255.252.0
LSRefreshTime is1800

Displayed information	Explanation
my router ID	The ID of the current layer 3 switch
preference	Routing protocol priority
ase perference	Exterior routes priority for introduction
export metric	The hops for output from the port
export tag	The route tag for output from the port
area ID interface count imes spf has been run for this area net range	OSPF area number: including statistics for interface number in the area, SPF algorithm calculation time and network scope.

（2）show ip route

The “show ip route” command can be used to display the information about OSPF routes in the route table: destination IP addresses, network masks, next hop IP addresses, and forwarding interfaces, etc.

For example, displayed information can be:

Switch#show ip route
Total route items is 4018, the matched route items is 4018
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived, D - DVMRP derived

	Destination	Mask	Nexthop	Interface	Preference
C	4.1.140.0	255.255.255.0	0.0.0.0	Vlan2139	0
A	5.1.1.0	255.255.255.0	12.1.1.2	Vlan12	150

A	5.1.2.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.3.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.4.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.5.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.6.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.7.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.8.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.9.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.10.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.11.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.12.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.13.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.14.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.15.0	255.255.255.0	12.1.1.2	Vlan12	150
A	5.1.16.0	255.255.255.0	12.1.1.2	Vlan12	150
O	5.1.17.0	255.255.255.0	12.1.1.2	Vlan12	110

---More---

Where, O stands for OSPF route, i.e., the OSPF route with the destination network address of 5.1.17.0, network mask of 255.255.255.0, the next hop address of 12.1.1.2 and the forwarding interface of Ethernet vlan12. The priority value of this route is 110.

（3）show ip ospf ase

The “show ip ospf ase” command can be used to display information about OSPF autonomous system exterior routes.

For example, displayed information can be:

Switch#show ip ospf ase

Destination	AdvRouter	NextHop	Age	SeqNumber	Type	Cost
10.1.1.125	11.11.1.2	11.1.1.2	3	300	2	20

Displayed information	Explanation
Destination	Target network segment or address
AdvRouter	Route election
NextHop	Next hop address
Age	Aging time
SeqNumber	Sequence number
Type	Exterior routes type for introduction
Cost	Cost for introducing exterior routes

（4）show ip ospf cumulative

The “show ip ospf cumulative” command can be used to display statistics about the OSPF protocol.

For example, displayed information can be:

Switch#show ip ospf cumulative

IO cumulative

type in out
HELLO 1048 253
DD 338 337
LS Req 62 219
LS Update 753 295
LS Ack 495 308
ASE count 0 checksum 0
original LSA 340 LS_RTR 179 LS_NET 1 LS_SUM_NET 160 LS_SUM_ASB 0 LS_ASE 0
received LSA 325
Areaid 0
nbr count 1 interface count 1
spf times 120
DB entry count 6
LS_RTR 2 LS_NET 2 LS_SUM_NET 3 LS_SUM_ASB 0 LS_ASE 3
Areaid 1
nbr count 2 interface count 1
spf times 52
DB entry count 6
LS_RTR 3 LS_NET 3 LS_SUM_NET 1 LS_SUM_ASB 0 LS_ASE 3
AS internal route 4 AS external route 0

Displayed information	Explanation
IO cumulative	Statistics for OSPF packets in/out.
type	Packet type: including HELLO packet, DD packet, LS request, update and acknowledging packet, etc.
In	Packet in statistics
Out	Packet out statistics
Areaid	OSPF statistics fro a specific OSPF area

（5）show ip ospf database

The “show ip ospf database” command can be used to display information about the link-state database for OSPF protocol.

For example, displayed information can be:

Switch#show ip ospf database
OSPF router ID：11.11.4.1 AS：No
Area 1>>>>>>>> Area ID： 0

Router LSAs

LS ID (Router ID)	ADV rtr	Age	Sequence	Cost	Checksum
11.11.4.1	11.11.4.1	0	2147483808	0	42401

11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Router LSA

11.11.4.1	11.11.4.1	0	2147483808	0	42401
11.11.4.2	11.11.4.2	18	2147483863	1	6777215

Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(DR's IP)					
11.11.4.2	11.11.4.2	1	2147483662	1	35126

Summary Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Net's IP)					
11.11.1.0	11.11.4.1	0	2147483656	1	6777215
11.11.2.255	11.11.4.1	0	2147483649	1	6777215
11.11.3.255	11.11.4.1	0	2147483680	1	6777215

ASBR Summary LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(ASBR's Rtr ID)					

Area 2>>>>>>>> Area ID： 1

Router LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(Router ID)					
11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875

Router LSA

11.11.2.1	11.11.2.1	1	2147483698	1	6777215
14.14.14.1	14.14.14.1	1	2147483662	1	14831
11.11.4.1	11.11.4.1	0	2147483669	0	33875

Network LSAs

LS ID	ADV rtr	Age	Sequence	Cost	Checksum
(DR's IP)					
11.11.1.1	11.11.4.1	0	2147483649	1	6777215

11.11.1.3 14.14.14.1 15 2147483705 1 53384

Summary Network LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(Net's IP)
11.11.4.255 11.11.4.1 0 2147483677 1 6777215

ASBR Summary LSAs

LS ID ADV rtr Age Sequence Cost Checksum
(ASBR's Rtr ID)

AS External LSAs

LS ID Route type ADV rtr Age Sequence Cost Checksu Forw addr RouteTag
(Ext Net's IP)

Displayed information	Explanation
OSPF router ID	The ID of the layer 3 switch
Area 1>>>>>>>> Area ID： 0	Represents the LSA database information from area 0 to area 0
Router LSAs	Route LSA
Network LSAs	Network LSA
Summary Network LSAs	Summary network LSA
ASBR Summary LSAs	Autonomous system exterior LSA

（6）show ip ospf interface

The “show ip ospf interface” command can be used to display the OSPF protocol information for the interface.

For example, displayed information can be:

Switch#show ip ospf interface vlan 1
IP address： 11.11.4.1 Mask： 255.255.255.0 Area： 0
Net type： BROADCAST cost： 1
State： IBACKUP Type： BDR
Priority： 1 Transit Delay： 1
DR： 11.11.4.2 BDR： 11.11.4.1
Authentication key：
Timer： Hello：10 Poll： 0 Dead： 40 Retrans： 5
Number of Neigbors： 1 Nubmer of Adjacencies： 1
Adjacencies：
1： 11.11.4.2

Displayed information	Explanation
IP address	Interface IP address
Mask	Interface mask.
Area	The area of the interface
Net type	Network type, such as broadcast, p2mp, etc.

cost	Cost value
State	Status
Type	Layer 3 switch type, such as designated
Priority	Configure the priority in electing designated layer 3 switch.
Transit Delay	The delay value for interface to transfer LAS
DR	The designated layer 3 switch
BDR	Backup designated layer 3 switch
Authentication key	OSPF packet authentication key
Timer： Hello, Poll, Dead, Retrans	OSPF protocol timer: including time set for HELLO packet, poll interval packet, route invalid, route retransmission, etc.
Number of Neigbors	The number of neighboring layer 3 switches
Nubmer of Adjacencies	The number of neighboring route interfaces
Adjacencies	Neighboring interface IP address

（7）show ip ospf neighbor

The “show ip ospf neighbor” command can be used to display information about the neighbor OSPF layer 3 switches.

For example, displayed information can be:

```
Switch#show ip ospf neighbor
interface ip 12.1.1.1       area id 0
   router id 12.1.1.2        router ip addr 12.1.1.2
   state NFULL       priority 1
   DR 12.1.1.2        BDR 12.1.1.1
   last hello 66261       last exch 65712
interface ip 30.1.1.1       area id 0
interface ip 50.1.1.1       area id 0
   router id 50.1.1.2        router ip addr 50.1.1.2
   state NFULL       priority 0
   DR 50.1.1.1        BDR 0.0.0.0
   last hello 66286       last exch 49614
interface ip 51.1.1.1       area id 0
interface ip 52.1.1.1       area id 0
interface ip 100.1.1.1       area id 0
interface ip 110.1.1.1       area id 0
interface ip 150.1.1.1       area id 0
   router id 12.2.0.0        router ip addr 150.1.1.2
   state NFULL       priority 0
   DR 150.1.1.1        BDR 0.0.0.0
   last hello 66289       last exch 49607
```

Displayed information	Explanation
interface ip	The IP address of an interface in the current layer 3 switch

area id	The id of the area for the interface
router id	The ID of the neighbor layer 3 switch
router ip addr	IP address of the neighboring layer 3 switch
state	Link-state status
priority	Priority
DR	ID of the designated layer 3 switch
BDR	ID of the backup designated layer 3 switch
last hello	The last HELLO packet
last exch	The last packet exchanged

（8）show ip ospf routing

The "show ip ospf routing" command can be used to display information about the OSPF route table.

For example, displayed information can be:

Switch#show ip ospf routing

AS internal routes：

Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
11.11.1.0	1	1	0	11.11.1.1	14.14.14.1
11.11.4.0	0	1	0	11.11.4.1	11.11.4.2
11.11.2.0	1	2	0	11.11.1.2	11.11.2.1
11.11.3.0	1	11	0	11.11.1.3	14.14.14.1

AS external routes：

Destination	Cost	Dest Type	Next Hop	ADV rtr

Displayed information	Explanation
AS internal routes	Autonomous system interior route
AS external routes	Autonomous system exterior route
Destination	Destination network segment
Area	Area number
Cost	Cost value
Dest Type	Route Type
Next Hop	Next hop
ADV rtr	Advertise the interface address of the layer 3 switch.

（9）show ip ospf virtual-links

The "show ip ospf virtual-links" command can be used to display information about the OSPF virtual link.

For example, displayed information can be:

Switch#show ip ospf virtual-links

no virtual-link

（10）show ip protocols

"show ip protocols" command can be used to display the information of the routing protocols running in the switch.

For example, displayed information can be:

Switch#sh ip protocols

OSPF is running.

my router ID is 100.1.1.1
preference=10 ase perference=150
export metric=1
export tag=-2147483648
area ID 1
interface count:2
7times spf has been run for this area
net range:
LSRefreshTime is1800
RIP information
rip is shutting down

Displayed information	Explanation
OSPF is running	The running routing protocol is OSPF protocol
My router ID	The ID number of the layer 3 switch running
Preference	OSPF routing priority
Ase perference	Autonomous system exterior routes priority
Export metric	Metrics for exporting OSPF routes
Export tag	Tag value for exporting OSPF routes
Area ID	The ID of the OSPF area where the current layer 3 switch resides
Interface count	Number of interface running OSPF routing protocol
N times spf has been run for this area	The number of times the layer 3 switch performs minimum tree spanning calculation.
Net range	The network scope for running OSPF protocol
LSRefreshTime	Link-state advertisement (LSA) update interval of OSPF protocol

18.4.4.2 OSPF Troubleshooting Help

In configuring and using OSPF protocol, the OSPF protocol may fail to run properly due to reasons such as physical connection failure or incorrect configuration. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interface” command).
- ✧ Then IP addresses of different network segments should be configured in all interfaces.
- ✧ Enable OSPF (use “router rip” command) first, then configure OSPF areas for appropriate interfaces to reside in.
- ✧ Next, note the nature of OSPF – OSPF backbone area (area 0) must be continuous, if not, use virtual link to make it continuous; all non-0 areas must connect to the others via area 0, direct connection between non-0 areas is not allowed; edge layer 3 switch refers to the layer 3 switch that partly belongs to area 0 and partly belong to non-0 area; for mutli-access network-like broadcast networks, designated layer 3 switch (DR) should be elected.

If OSPF routing problems persist after the above-mentioned procedures, please run debugging commands like “debug ip ospf packet” and “event”, and copy the debug information in 3 minute and send the information to Edge-Core technical service center.

18.5 WEB MANAGEMENT

Click “Route configuration” to open “routing protocol configuration” to configure the items as follows:

- Static route configuration
- RIP configuration
- OSPF configuration
- Show ip route

18.5.1 Static route

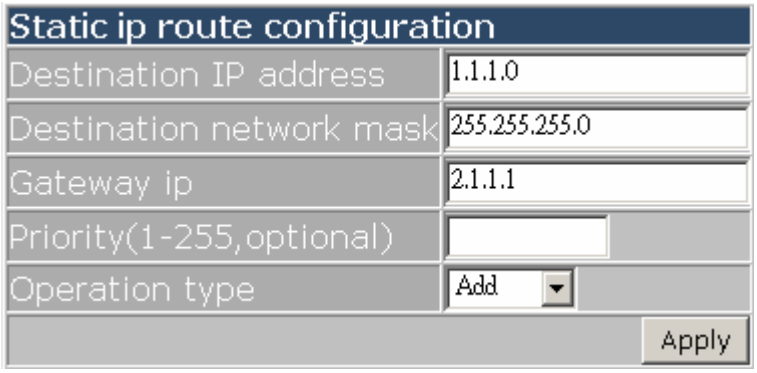
Click “Static route configuration” to configure static route

18.5.1.1 Static route configuration

Click “Static route configuration” to enter the configuration page. Equivalent to CLI command 18.2.3.2.1 including.

- Destination IP address
- Destination network mask
- Gateway ip: the IP address of next-hop
- Priority: routing priority level
- Operation type: Add or Remove

Example: Adding a static route. Enter the destination IP as 1.1.1.0, mask as 255.255.255.0, gateway as 2.1.1.1. select Add then click Apply button.



18.5.2 RIP configuration

Click RIP configuration to open RIP configuration including:

- Enable RIP: enable RIP including
  - ✓ Enable RIP: enable
  - ✓ Enable port to receive/transmit RIP packet
- RIP parameter configuration (optional) including:
  - ✓ Enable imported route
  - ✓ Metricin/out configuration

- ✓ RIP port imported route
- ✓ RIP mode configuration
- ✓ RIP timer configuration

18.5.2.1 RIP configuration

18.5.2.1.1 Enable RIP

Click “Enable RIP” to enter configuration page. Equivalent to CLI command 18.3.2.2.17.

- Enable RIP: Enables RIP and Disables RIP

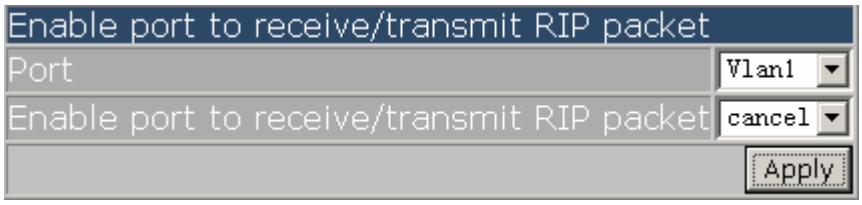
Example: Select Enable RIP and click Apply button to enable RIP.

18.5.2.1.2 Enable port to receive/transmit RIP packet

Click “Enable port” to enter configuration page for receiving/transmitting RIP packet. Equivalent to CLI command 18.3.2.2.11

- Port: specify port
- Enable port to receive/transmit RIP packet: set or cancel

Example: Select port valn1 and cancel. Click Apply to cancel receive/transmit packets on vlan1



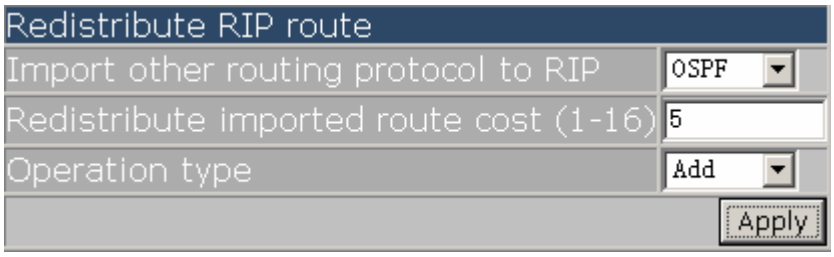
18.5.2.2 RIP parameter configuration

18.5.2.2.1 Enable imported route

Click “Enable imported route” to enter the configuration page. Equivalent to CLI command 18.3.2.2.13

- Import other routing protocol to RIP: includes Static, OSPF, BGP
- Redistribute imported route cost
- Operation type: Add or Remove

Example: For protocol select OSPF, cost as 5, then select Add. Click Apply button to redistribute imported route cost 5 with OSPF routing protocol to RIP.

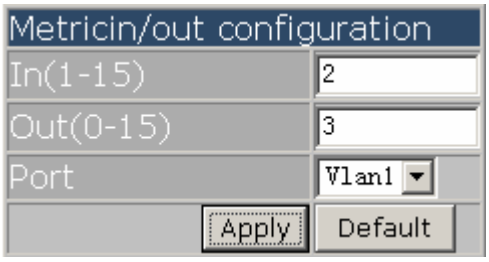


18.5.2.2.2 Metricin/out configuration

Click "Metricin/out configuration" to enter the configuration page

- In: the value of metric in. Equivalent to CLI command 18.3.2.2.5
- Out: the vale of metric out. Equivalent to CLI command 18.3.2.2.6
- Port: specifies port
- Apply: valid settings in this page
- Default: default settings

Example: Configuring metric in/out value, key in the value in In/Out columns, select port.

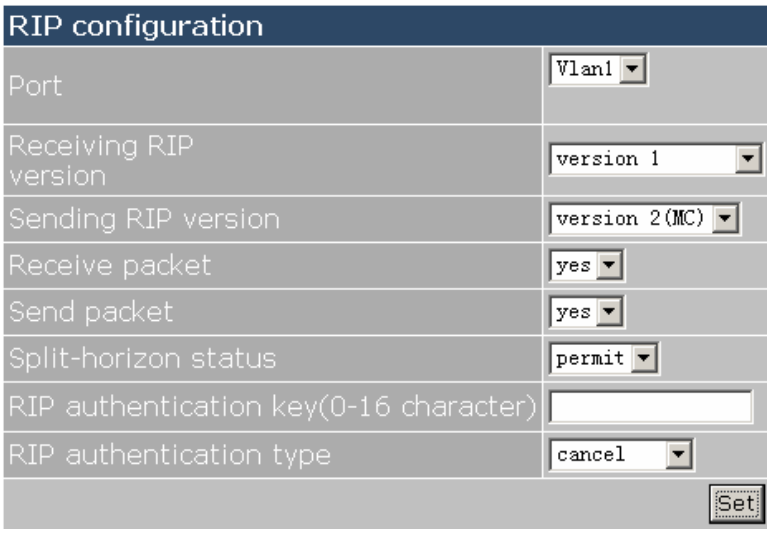


18.5.2.2.3 RIP imported route

Click "RIP port imported route" to enter the configuration page

- Port: specifies port
- Receiving RIP version: sets up port receiving RIP version. Includes version1, version2 and version 1 and 2. It is equivalent CLI command 18.3.2.2.9.
- Sending RIP version: sets up port sending RIP version, including version1, version2 (BC) andversion2 (MC). Equivalent to CLI command 18.3.2.2.10
- Receive packet: sets up whether the port will receive RIP packet or not, including yes and no. Equivalent to CLI command 18.3.2.2.7
- Send packet: sets up whether the port will send RIP packets or not. Equivalent to CLI command 18.3.2.2.8
- Split-horizon status: sets up split-horizon status, including permit and forbid. Equivalent to CLI command 18.3.2.2.12
- RIP authentication key: Sets up RIP authentication key. Equivalent to CLI command 18.3.2.2.3
- RIP authentication type: sets up RIP authentication type. Text means text authentication; md5 means normal MD5 authentication; Cisco MD5 means Cisco MD5 authentication; cancel means back to default. Equivalent to CLI command 18.3.2.2.4.

Example:

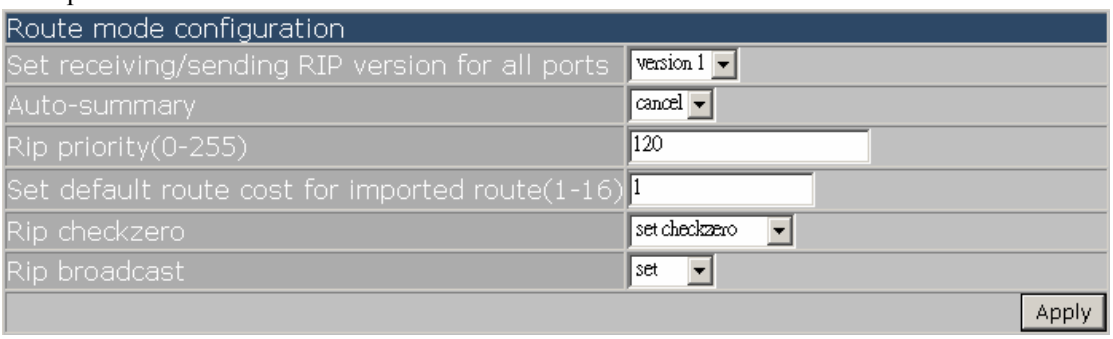


18.5.2.2.4 Global RIP configuration

Click "RIP mode configuration" to enter the configuration page.

- Set receiving/sending RIP version for all ports: sets up receiving/sending RIP version for all port, including version1, version2 and Cancel means default. Equivalent to CLI command 18.3.2.2.19
- Auto-summary: configures route aggregate function including set and cancel. Equivalent to CLI command 18.3.2.2.1
- Rip priority (0-255): sets up the route priority level of RIP protocol. Equivalent to CLI command 18.3.2.2.16
- Set default route cost for imported route (1-16): sets up default route cost for imported route value. Equivalent to CLI command 18.3.2.2.2
- Rip checkzero: sets up check zero of RIP packet, including set and cancel. Equivalent to CLI command 18.3.2.2.15
- Rip broadcast: sets up all ports send RIP BC or MC packets of the L3 switch, including set and cancel. Equivalent to CLI command 18.3.2.2.14

Example:

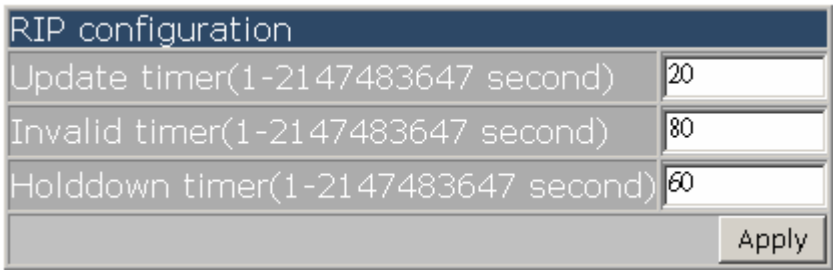


18.5.2.2.5 Set RIP timer

Click “RIP timer configuration” to enter the configuration page. Equivalent to CLI command 18.3.2.2.18

- Update time: sending update packet time interval
- Invalid timer: RIP route invalid time
- Holddown timer: specified invalid routes existing interval in the routing table

Example:



18.5.3 OSPF

Click “OSPF configuration” to open OSPF configuration. Includes:

- OSPF enable: enables OSPF protocol
- OSPF TX-parameter configuration: configures OSPF forwarding packet parameter
- Imported route parameter configuration: configures OSPF imported route parameter
- Other parameter configuration: configures other parameter of OSPG protocol
- OSPF debug: OSPF debugging message.

18.5.3.1 Enable OSPF protocol

Click “OSPF enable” to open the configuration table. Includes:

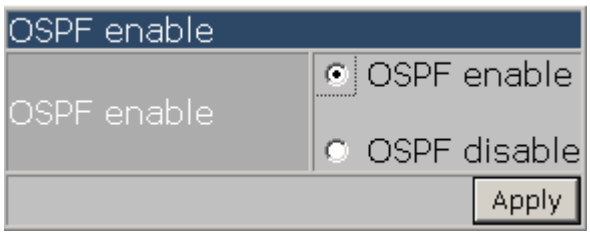
- OSPF enable: enables/disables OSPF protocol
- Router-ID configuration: configures the router ID number of the OSPF protocol
- OSPF network range configuration: configures OSPF network range of OSPF
- OSPF area configuration for port: configures OSPF area for port

18.5.3.1.1 Enable/Disable OSPF protocol

Click “OSPF enable” to enter the configuration page. Equivalent to CLI command 18.4.2.2.19.

- OSPF enable: select from OSPF enable or OSPF disable
- Reset: clears selection

Example: Select OSPF enable and click Apply button to enable OSPF protocol

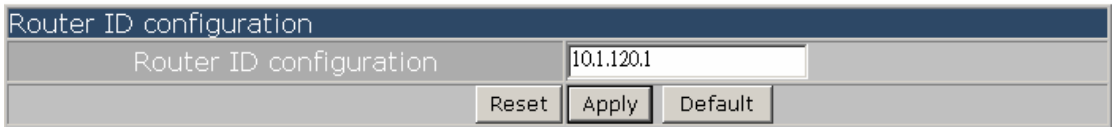


18.5.3.1.2 Router-ID configuration

Click "Router-ID configuration" to enter the configuration page. Equivalent to CLI command 18.4.2.2.18

- Router-ID configuration: ID number
- Reset: clears key-in parameter
- Apply: configures Router-ID number
- Default: deletes the ID number of the Layer 3 switch

Example:

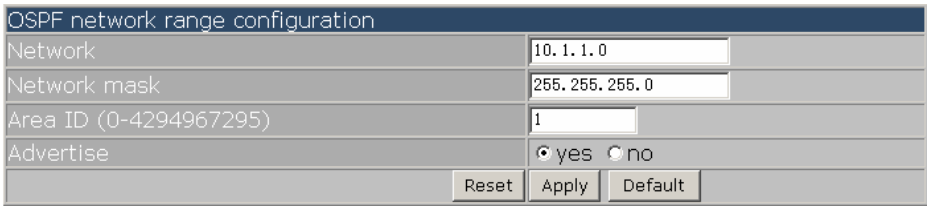


18.5.3.1.3 OSPF network range configuration

Click "OSPF network range configuration" to enter the configuration page. Equivalent to CLI command 18.4.2.2.15

- Network: network IP address
- Network mask: mask
- Area ID: area number
- Advertise: specify whether broadcast the brief message of this network range or not, including yes and no.
- Reset: reset each column value to default in this page and this action will not change settings
- Apply: valid each column value and this action will change settings
- Default: back to default setting and this action will change settings

Example: To define network range 10.1.1.0 255.255.255.0 to add into area 1, key-in 10.1.1.0 in network, 255.255.255.0 into mask, 1 into ID and select yes and click Apply button to complete the action

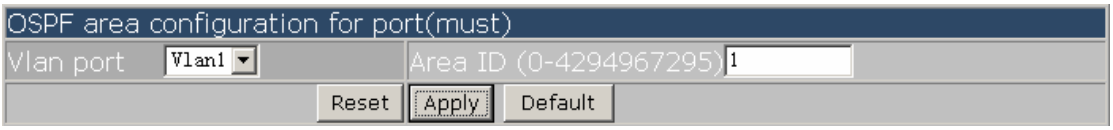


18.5.3.1.4 Configure OSPF area for port

Click “OSPF area configuration” to enter the configuration page for port. Equivalent to CLI command 18.4.2.2.9

- Vlan port: port list
- Area ID: area number
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings.
- Default: resets to default setting. This action will change settings.

Example: to configure port vlan 1 to area 1, port select vlan 1, key-in area number 1 and click Apply button.



18.5.3.2 OSPF TX-parameter configuration

Click “OSPF Tx-parameter configuration” to open the configuration table. Includes:

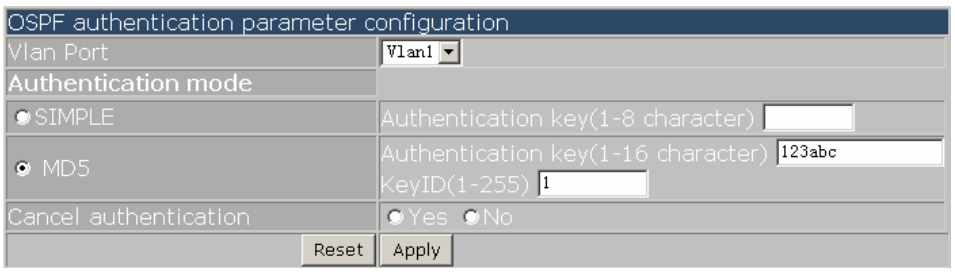
- OSPF authentication parameter configuration
- Passive interface configuration: Configures OSPF port as receiving packets only
- Sending packet cost configuration: configures the cost and timer parameter for the port sending data packets.

18.5.3.2.1 Configure OSPF authentication parameter configuration

Click “OSPF authentication parameter configuration” to enter the configuration page. Equivalent to CLI command 18.4.2.2.6

- Vlan port: port list
- Authentication mode: simple and MD5.
- Authentication key
- KeyID: the authentication word in MD5 authentication mode
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value and this action will change settings

Example: To configure MD5 authentication mode in port vlan 1, authentication key as 123abc and the key ID as 1: select vlan1, MD5 and key-in authentication key as 123abc and key ID as 1.

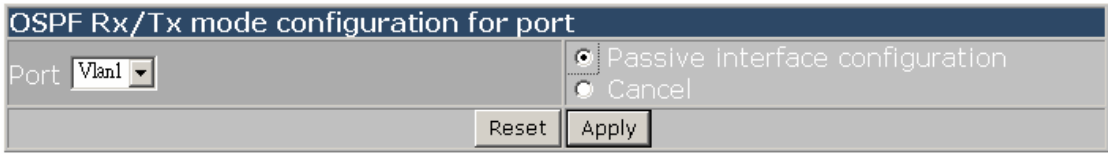


18.5.3.2.2 Passive interface configuration

Click “Passive interface configuration” to enter the configuration page. Equivalent to CLI command 18.4.2.2.11.

- Port: port list
- Passive interface configuration: sets up to receive OSPF packets only
- Cancel: cancels the setting.
- Reset: resets to default parameters

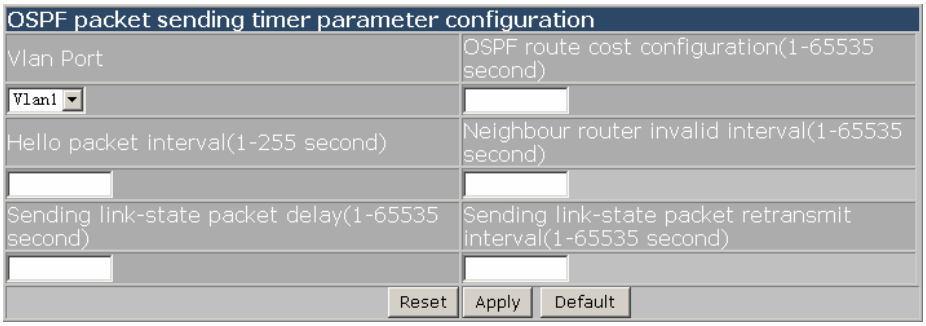
Example: Select port vlan1, select Passive interface configuration and click Apply button to configure port vlan 1 as receiving OSPF packet only.



18.5.3.2.3 Sending packet cost configuration

Click “Sending packet cost configuration” to enter the configuration page.

- Vlan port: port list
- OSPF route cost configuration: specifies the cost needed for the OSPF protocol port. Equivalent to CLI command 18.4.2.2.7
- Hello packet interval: specifies the interval time to send a hello packet on the ports. Equivalent to CLI command 18.4.2.2.10
- Neighbor router invalid interval: specifies the invalid time length for neighboring Layer 3 switches. Equivalent to CLI command 18.4.2.2.8
- Sending link-state packet delay: sets up the value of Sending link-state packet delay on ports. Equals to CLI command 18.4.2.2.14
- Sending link-state packet retransmit interval: specifies the Sending link-state packet retransmit interval of the port with neighbor L3 switch. Equivalent to CLI command 18.4.2.2.13
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings
- Default: resets to default settings. This action will change settings



18.5.3.3 OSPF imported route parameter configuration

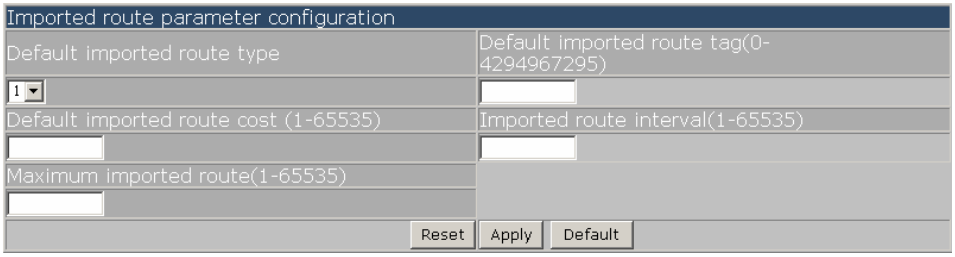
Click “OSPF Imported route parameter configuration” to open the configuration table, includes:

- Imported route parameter configuration: configure imported route default parameter
- Import external routing information: configure other imported protocol in OSPF

18.5.3.3.1 Imported route parameter configuration

Click “Imported route parameter configuration” to enter the configuration page.

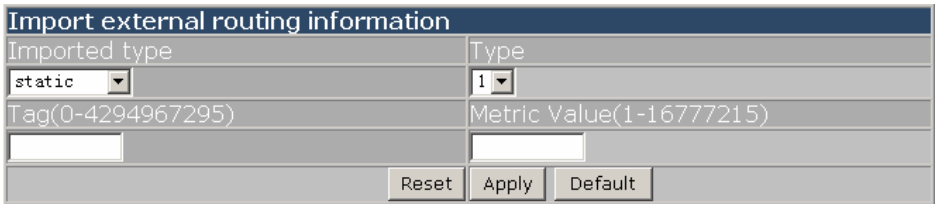
- Default imported route type: default imported route type. 1 means the first type external route and 2 means the second type external route. Equivalent to CLI command 18.4.2.2.5
- Default imported route tag: default imported route tag. Equivalent to CLI command 18.4.2.2.4
- Default imported route cost: Default imported route cost. Equivalent to CLI command 18.4.2.2.1
- Imported route interval: imported route interval. Equivalent to CLI command 18.4.2.2.2
- Maximum imported route: maximum imported route at once. Equivalent to CLI command 18.4.2.2.3
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings.
- Default: resets to default settings. This action will change settings.



18.5.3.3.2 Import external routing information

Click “Import external routing information” to enter configuration page. Equivalent to CLI command 18.4.2.2.17

- Imported type: includes Static, RIP, connected direct route and BGP as external route information
- Type: specify external route type, 1 means the first type external route and 2 means the second type external route
- Tag: specifies route tag
- Metric value: specifies route value
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings.
- Default: resets to default settings. This action will change settings.



18.5.3.4 Other parameter configuration

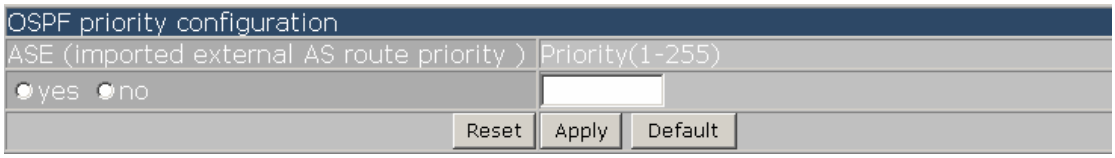
Click “Other parameter configuration” to open the configuration table including:

- OSPF priority configuration: configures OSPF routing protocol priority level
- OSPF STUB area and default route cost: configures OSPF STUB area and default route cost
- OSPF virtual link configuration: configures OSPF virtual link
- Port DR priority configuration: configures port DR priority in selected Layer 3 switch

18.5.3.4.1 OSPF priority configuration

Click “OSPF priority configuration” to enter the configuration page. Equivalent to CLI command 18.4.2.2.16

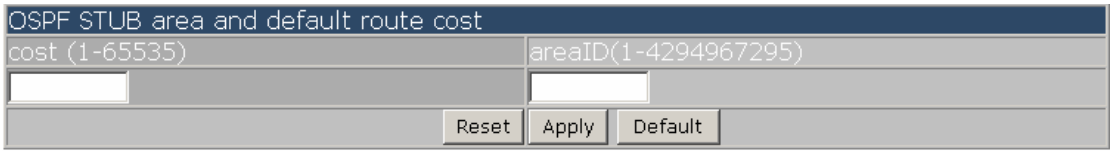
- ASE: yes means the priority level of specified imported OSPF external route; no means the priority level for specified OSPF protocol in all routes
- Priority: priority level
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings
- Default: resets to default setting. This action will change settings



18.5.3.4.2 OSPF STUB area and default route cost configuration

Click “OSPF STUB area” and “default route cost” to enter the configuration page. Equivalent to CLI command 18.4.2.2.20

- Cost: stub area default routing cost value
- areaID: stub area number
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings
- Default: resets to default setting. This action will change settings

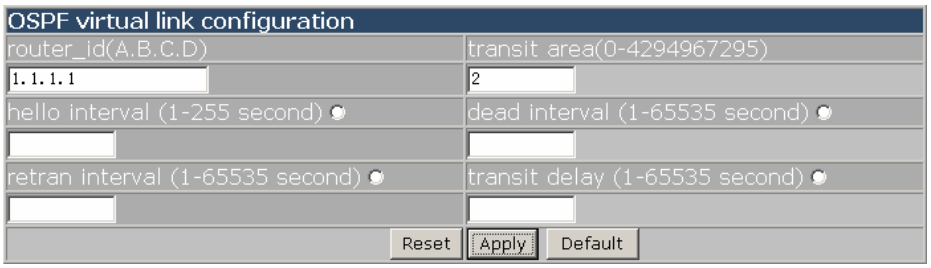


18.5.3.4.3 OSPF virtual link configuration

Click “OSPF virtual link configuration” to enter the configuration page. Equivalent to CLI command 8.4.2.2.21

- router_id: neighbor virtual lick ID
- transit area: transit area number
- hello interval: sending hello packet time interval

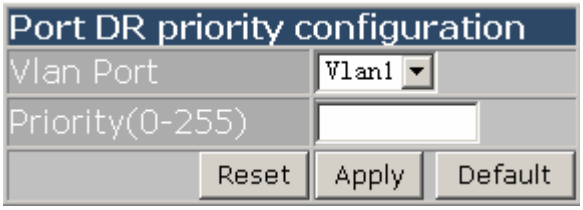
- dead interval: invalid route time interval
- retran interval: sending LSA retran interval
- transit delay: sending LSA transit delay
- Reset: resets each column value to default in this page and this action will not change settings
- Apply: valid each column value. This action will change settings
- Default: resets to default setting. This action will change settings



18.5.3.4.4 Port DR priority configuration

Click “Port DR priority configuration” to enter the configuration page. Equivalent to CLI command 18.4.2.2.12

- Vlan Port
- Priority



18.5.3.5 OSPF debug

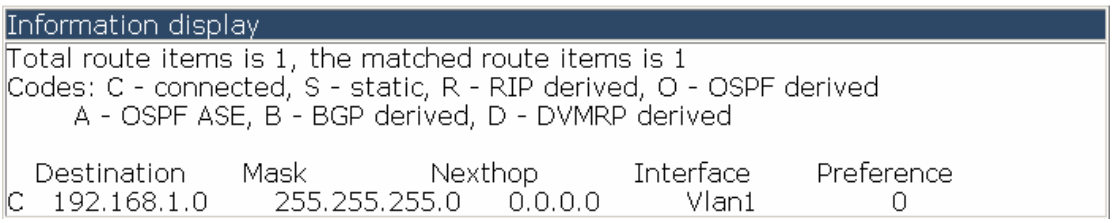
Click “OSPF debug” to open configuration table including:

- show ip ospf: displays OSPF main information. Equivalent to CLI command 18.4.2.2.22
- show ip ospf ase: displays OSPF external route information. Equivalent to CLI command 18.4.2.2.23
- show ip ospf cumulative: displays OSPF statistic information. Equivalent to CLI command 18.4.2.2.24
- show ip ospf database: displays OSPF link status data information. Equivalent to CLI command 18.4.2.2.25
- show ip ospf interface: displays OSPF interface information. Equivalent to CLI command 18.4.2.2.26
- show ip ospf neighbor: displays OSPF neighbor node information. Equivalent to CLI command 18.4.2.2. 27
- show ip ospf routing: displays OSPF routing table information. Equivalent to CLI command 18.4.2.2. 28
- show ip ospf virtual-links: displays OSPF virtual link information. Equivalent to CLI command 18.4.2.2.29
- show ip protocols: displays current routing protocol information of the L3 switch. Equivalent to CLI command 18.4.2.2.30.

Click the related nodes to check display information

18.5.4 Display routing table

Click “Show ip route” to display the routing table.


Information display
Total route items is 1, the matched route items is 1
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
A - OSPF ASE, B - BGP derived, D - DVMRP derived
Destination Mask Nexthop Interface Preference
C 192.168.1.0 255.255.255.0 0.0.0.0 Vlan1 0

Chapter 19 Multicast protocol Configuration

19.1 Multicast Protocol Overview

19.1.1 Introduction to Multicast

When sending information (including data, voice and video) to a small number of users in the network, there are several ways of transmission. For example, the unicast method that establishes a separate data transmission channel for each user and the broadcast method which sends information to all users in the network regardless of whether they need the information or not. Suppose 200 users in a network need to receive the same information, traditionally, the unicast method is employed to sends the same information 200 times to ensure users requiring the data can get what they need; or the information is broadcasted throughout the network so that users requiring the data can obtain what they need directly from the network. Both methods waste a large amount of precious bandwidth resource, and the broadcast method is unfavorable for security of information.

The advent of IP multicast technology solved this problem. Multicast source sends the information only once, and the multicast routing protocol create a tree route for the multicast packet; the information being transferred will start duplicating and distribution in the fork as fast as possible. This way, the information can be sent to each user requiring it accurately and efficiently.

It should be noted that the multicast source is not necessarily a member of the multicast group. When sending data to some multicast group, the sender itself is not necessarily a receiver of that group. Multiple sources are allowed to send packets to the same multicast group at the same time. There may be routers not support multicast in the network. Multicast routers can transfer the multicast packets encapsulated in unicast IP packets in tunnel mode to the neighbor multicast routes, the neighbor multicast routers will strip the unicast IP head can continue multicast transmission. This way, large modification to the network structure can be avoided. The major benefits of multicast are:

1) Improved efficiency and reduced network traffic and server/CPU load.
2) Improved performance and reduced unnecessary traffic.
3) Distributed application: enabling multiple point application.

19.1.2 Multicast Address

The multicast packets uses Class D IP address as their destination addresses, ranging from 224.0.0.0 to 239.255.255.255. Class D addresses cannot be used in the source IP address field of an IP packet. In unicast, the path a packet travels is from the source address to the destination address, and the packet is transfer in the network hop-by-hop. However, in IP multicast, the destination address of a packet is a group (group address) instead of one single address. All information receivers are arranged in the same group. And once a receiver joins a multicast group, data sent to multicast address will immediately start transferring to the receiver. All members in the group will receive the packets. The membership for a multicast group is dynamic; the hosts can join and quit a multicast

group at any time.

A multicast group can be either a perpetual one or temporary one. Part of multicast addresses are assigned officially and referred to as the perpetual multicast group. The IP address of a perpetual multicast group remains the same, but the membership can be changed. A perpetual multicast group can have any number of members, even zero. IP multicast addresses not reserved for perpetual multicast group can be used by temporary multicast groups.

224.0.0.0 – 224.0.0.255 are reserved multicast addresses (perpetual group address), the address 224.0.0.0 is not used, the other addresses are available for routing protocols; 224.0.1.0 – 238.255.255.255 are multicast addresses available to users (temporary group address), and is valid for the whole network; 239.0.0.0 – 239.255.255.255 are local administrative multicast address and is valid for specific local ranges. The following is a list for common reserved multicast addresses:

224.0.0.0 Base address (reserved)
224.0.0.1 All-host address
224.0.0.2 All-multicast-router address
224.0.0.3 Not for allocation
224.0.0.4 DVMRP router
224.0.0.5 OSPF router
224.0.0.6 OSPF DR
224.0.0.7 ST router
224.0.0.7 ST host
224.0.0.9 RIP-II router
224.0.0.10 IGRP router
224.0.0.11 Active proxy
224.0.0.12 DHCP Server/Relay proxy
224.0.0.13 All PIM routers
224.0.0.14 RSVP packaging
224.0.0.15 All CBT routers
224.0.0.16 Specified SBM
224.0.0.17 All SBMS
224.0.0.18 VRRP

When transferring unicast IP packets on Ethernet, the destination MAC address is the MAC of the receiver. However, in transferring multicast packets, as the destination is no longer one specific recipient but a group with unknown members, the destination address used is the multicast MAC address. Multicast MAC address is corresponding 5 to the multicast IP address. According to IANA (Internet Assigned Number Authority), the 24 MSbs of multicast MAC is 0x01005e and 23 LSbs of multicast MAC is the same of the multicast IP address.

As only 23 bits out of the 28 LSbs of multicast IP address are mapped to MAC address, for one MAC address there will be 32 corresponding multicast IP addresses.

19.1.3 IP Multicast Packets Forwarding

In the multicast model, the source host sends information to the host group represented by the multicast group address in the destination address field of the IP packet. The multicast model differs from the unicast model in that a multicast packet must be forwarded to several external interfaces to send the packet to all receiving stations, i.e., multicast forwarding is more complex than unicast forwarding.

To ensure the multicast packets reach the routers using the shortest route, the multicast protocols must check the receiving interfaces of the multicast packets against the unicast route table or route table dedicated for multicast (such as a DVMRP route table). This checking mechanism is the base for most multicast routing protocols to perform forwarding, and is called Reverse Path Forwarding (RPF). Multicast routers use the source address of an arrived multicast packet to query the unicast route table or an independent multicast route table to make sure the ingress interface from which the packet arrived is in the shortest route from the receiving station to the source address. If an active tree is used, the source address is the address of source host sending the multicast packet; if a shared tree is used, the source address is the root address of that shared tree. When a multicast packet arrives at a router, the packet will be forwarded according to the multicast forwarding rules if the RPF check is ok; otherwise, the packet will be discarded.

19.1.4 Application of Multicast

IP multicast technology effectively solved the problem of one sender vs. multiple receivers, fulfilling the high efficiency data transmission from one point to multiple points in the IP network, and can significantly save the network bandwidth and reduce network traffic. The multicast feature can be conveniently used to provide some new value-added services, including online live broadcast, network TV, remote education, remote medical service, network radio, real-time video/audio meeting that can be summarized in the following three fields:

1) Multimedia and stream applications.
2) Data warehouse and financial (like stocks) applications.
3) Any point-to-multiple-points data distribution applications.

With the increasing of multimedia services in the IP network, multicast represents great market potential, and multicast service is widely used and spreading quickly.

19.2 Common Multicast Configurations

19.2.1 Common Multicast Configuration Commands

- **show ip mroute**

19.2.1.1 show ip mroute

Command: show ip mroute [*group_address*] [*source_address*]

Function: Displays the IP multicast packet forwarding entries.

Parameters: [*group_address*] specifies the group address for the forwarding entry to be displayed; **[*source_address*]** specifies the source address for the forwarding entry to be displayed

Default: No display by default.

Command mode: Admin Mode

Usage Guide: This command is used to display IP multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example: Displaying all IP multicast forwarding entries.

Switch # **show ip mroute**

Name: Loopback, Index: 2001, State:9 localaddr: 127.0.0.1, remote: 127.0.0.1

Name: Vlan1, Index: 2005, State:13 localaddr: 1.1.1.1, remote: 1.1.1.1

Name: Vlan4, Index: 2006, State:13 localaddr: 2.1.1.1, remote: 2.1.1.1

Name: Vlan3, Index: 2007, State:13 localaddr: 3.1.1.1, remote: 3.1.1.1

Group	Origin	Iif	Wrong	Oif:TTL
225.1.1.101	1.1.1.100	Vlan1	0	2006:1
				2007:1
239.255.0.1	9.1.1.100	Vlan4	0	2005:1
239.255.0.1	7.1.1.100	Vlan4	0	2005:1
239.255.0.1	1.1.1.100	Vlan1	0	2006:1
				2007:1

Switch #

Displayed information	Explanation
Name	The interface list used by the multicast protocol and basic information for the interfaces
Index	Index number for the interface
Group	Multicast forwarding entry group address
Origin	Multicast forwarding entry source address
Iif	Multicast forwarding entry ingress interface
Wrong	The number of multicast packets (to this forwarding entry) from wrong incoming interfaces
Oif:TTL	Oif stands for the outgoing interface list, this list can be referred to by the index number according to the information list above; TTL is the threshold value for that outgoing interface.

19.3 PIM-DM

19.3.1 Introduction to PIM-DM

PIM-DM (Protocol Independent Multicast，Dense Mode) is a dense mode multicast protocol. It is good for use in small networks as the multicast group members are relatively concentrated in such network environments.

The work process of PIM-DM can be summarized as the following phases: neighbor discovery, flooding & prune, grafting.

1. Neighbor discovery

PIM-DM routers need discover neighbors with HELLO packets on start up. Network nodes running PIM-DM keeps contact with HELLO packets. The HELLO packets are sent in regular intervals.

2. Flooding and Prune

PIM-DM assumes all hosts in the network are ready for receiving multicast data. When a multicast source S starts sending data to multicast group G, the router will first perform RPF check against the unicast route table to the multicast packet. If check is ok, the router will create a (S, G) entry and forward the multicast packet to all downstream PIM-DM nodes in the network (Flooding). If RPF check fails, indicating the multicast packet is coming from the wrong interface, the packet will be discarded. After this process, each node in the PIM-DM multicast domain will create a (S, G) entry. If no multicast group member exists in the downstream nodes, then a prune message will be sent to the upstream nodes to inform the upstream node that no more forwarding for that multicast group is necessary. The upstream nodes will delete the corresponding interface, multicast forwarding entry (S,G), from the outgoing interface list. Hence a shortest path tree (SPT) rooted by source S is established. The prune process is initiated by leaf routers first.

The above procedures are referred to as the Flooding-Prune process. A timeout mechanism is provided for each pruned nodes, when the prune times out, the router restarts the flooding-prune process. The PIM-DM flooding-prune process is performed in regular intervals.

3. RPF check

PIM-DM employs the RPF check method to build a multicast tree rooted from the data source according to the existing unicast route table. When a multicast arrives at the router, its path correctness is checked first. If as indicated by the unicast route, the arriving interface is the interface to the multicast source, the packet is considered to be from the correct path; otherwise, the multicast packet is discarded as a redundant packet. The unicast route information used as the route decision fact is not dependent on specific unicast routing protocol, but can be the route information of any unicast routing protocols, such as route discovered by RIP, OSPF, etc.

4. Assert mechanism

If two routers (A and B) in the same LAN segment both have a receiving path to multicast source S, both will forward the multicast packet sent by multicast source S in the LAN. As a result, the downstream multicast router C will receive two identical multicast packets. On detecting such situation, the router will decide a unique forwarder through the Assert mechanism. The best forwarding path is decided by sending Assert packets. If two or more paths have the same priority and costs, then the node with a larger IP address is selected as the upstream neighbor for the (S, G) entry and is responsible for the forwarding of multicast packet for that (S, G) entry.

5. Graft

If a pruned downstream node needs to restore to the forwarding state, the node will send a graft packet to ask the upstream to restore multicast data forwarding.

19.3.2 PIM-DM Configuration

19.3.2.1 PIM-DM Configuration Task Sequence

1. Enable PIM-DM

Basic configuration of PIM-DM routing protocol on ES4704BD series switches is quite simple: just enable PIM-DM in the appropriate interfaces.

Command	Explanation
Interface Mode	
ip pim dense-mode **no ip pim dense-mode**	Enables PIM-DM protocol; the "**no ip pim dense-mode**" command disables PIM-DM protocol (required)

2. Configure PIM-DM sub-parameters

(1) Configure PIM-DM interface parameters

a. Configure PIM-DM HELLO packet interval

Command	Explanation
Interface Mode	
ip pim query-interval <*query interval*> **no ip pim query-interval**	Sets the interval for sending PIM-DM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

3. Disable PIM-DM protocol

Command	Explanation
Interface Mode	
no ip pim dense-mode	Disables PIM-DM protocol

19.3.2.2 PIM-DM Configuration Commands

- **ip pim dense-mode**
- **ip pim query-interval**
- **show ip pim interface**
- **show ip pim mroute dm**
- **show ip pim neighbor**
- **debug ip pim**
-

19.3.2.3 ip pim dense-mode

Command: ip pim dense-mode

no ip pim dense-mode

Function: Enables PIM-DM protocol on the interface; the "**no ip pim dense-mode**" command disables PIM-DM protocol on the interface.

Parameters: N/A.

Default: PIM-DM protocol is disabled by default.

Command mode: Interface Mode

Usage Guide:

Example: Enabling PIM-DM protocol on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim dense-mode

19.3.2.4 ip pim query-interval

Command: ip pim query-interval <*query interval*>

no ip pim query-interval

Function: Sets interval for sending PIM-DM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

Parameters: <***query interval***> is the interval for sending PIM-DM HELLO packets, ranging from 1 to 18724s.

Default: The default interval for sending PIM-DM HELLO is 10 seconds.econds.

Command mode: Interface Mode

Usage Guide: The HELLO message enables PIM-DM switches to locate each other and establish the neighborhood. PIM-DM switches claim their existence by sending HELLO message to their neighbors. If no HELLO message from a neighbor is received in a specified period, that neighbor is considered to be lost. This time must be no greater than the neighbor timeout time.

Example: Configuring PIM-DM HELLO interval on interface vlan1.

Switch (Config)#interface vlan1

Switch(Config-If-Vlan1)#ip pim query-interval 20

19.3.3 Typical PIM-DM Scenario

As shown in the figure below, the Ethernet interfaces of SwitchA and SwitchB are added to the appropriate vlan, and PIM-DM protocol is enabled on each vlan interface.

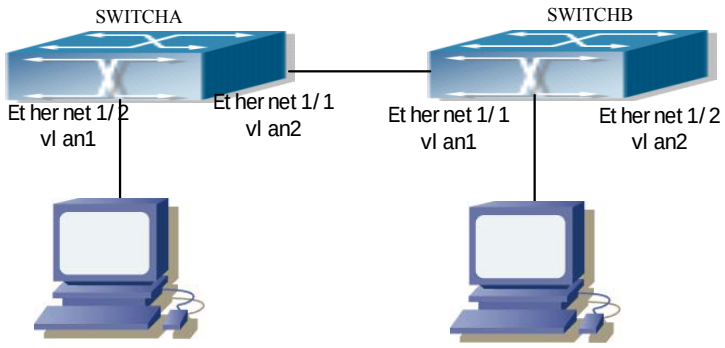


Fig 19-1 Typical PIM-DM environment

The followings are the configurations of SwitchA and SwitchB.

(1) Configuration of SwitchA:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim dense-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan2

Switch(Config-If-Vlan1)# ip pim dense-mode

(2) Configuration of SwitchB:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim dense-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan1)# ip pim dense-mode

19.3.4 PIM-DM Troubleshooting Help

1. Monitor and Debug Commands

2. PIM-DM Troubleshooting Help

19.3.4.1 Monitor and Debug Commands

Command	Explanation
Admin Mode	
show ip pim mroute dm	Displays the PIM-DM packet forwarding entry
show ip pim neighbor	Displays PIM-DM neighbor information
show ip pim interface	Displays PIM-DM interface information

debug ip pim	Enables the debugging function for displaying detailed PIM information; the "**no**" format of this command disables this debug function.

19.3.4.2 show ip pim mroute dm

Command: show ip pim mroute dm

Function: Displays the PIM-DM packet forwarding entry

Parameters: N/A.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: This command is used to display PIM-DM multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example: Displaying all PIM-DM packet forwarding entries.

Switch#sh ip pim mroute dm

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

PIMDM Group Table, inodes 7 routes 4:

(5.1.1.100, 225.0.0.1), protos: 0x8, flags: 0x4, 00:22:21/00:03:30
Incoming interface : Vlan3, RPF Nbr 0.0.0.0, pref 0, metric 0
Outgoing interface list:
(Vlan1), protos: 0x2, UpTime: 00:22:21, Exp:/
Prune interface list:
(Vlan2), protos: 0x2, UpTime: 00:22:21, Exp: 00:03:07

(5.1.1.100, 225.0.0.2), protos: 0x8, flags: 0x4, 00:18:52/00:03:30
Incoming interface : Vlan3, RPF Nbr 0.0.0.0, pref 0, metric 0
Outgoing interface list:
(Vlan1), protos: 0x2, UpTime: 00:18:52, Exp:/
Prune interface list:
(Vlan2), protos: 0x2, UpTime: 00:18:52, Exp: 00:02:51
Switch#

Displayed information	Explanation
(5.1.1.100, 225.0.0.1)	Forwarding entry
Incoming interface	Incoming interface or RPF interface

Outgoing interface list	Outgoing interface list.
Prune interface list	Downstream prune interface list.

19.3.4.3 show ip pim neighbor

Command: show ip pim neighbor [<*ifname*>]

Function: Displays information for neighbors of the PIM interface.

Parameters: **<*ifname*>** is the interface name, i.e., displays PIM neighbor information of the specified interface.

Default: PIM neighbor information is displayed by default on all interfaces.

Command mode: Admin Mode

Usage Guide: If no interface name is specified, then neighbor information for all interfaces will be displayed.

Example: Displaying neighbor information for all interfaces (do not specify the interface name)

```
Switch#sh ip pim neighbor
Neighbor-Address Interface      ifIndex Uptime    Expires   DR-state
 2.1.1.1         Vlan1          2005    00:25:17 00:01:15 /
 9.1.1.6         Vlan2          2006    00:25:09 00:01:35 DR
 5.1.1.4         Vlan3          2007    00:25:01 00:01:38 DR
Switch#
```

Displayed information	Explanation
Neighbor-Address	Neighbor address
Interface	The neighbor interface discovered.
ifIndex	Interface index number
Uptime	The up time of the neighbor since discovery
Expires	The remaining time before considering the neighbor to be invalid
DR-state	Whether the neighbor is a DR

19.3.4.4 show ip pim interface

Command: show ip pim interface [<*ifname*>]

Function: Displays information for the PIM interface.

Parameters: **<*ifname*>** is the interface name, i.e., display PIM information of the specified interface.

Default: PIM information is displayed by default on all interfaces.

Command mode: Admin Mode

Example: Displays PIM information of interface vlan 1.

```
Switch#sh ip pim interface vlan 1
Interface Vlan1 : 2.1.1.2
  owner is pimdm, Vif is 1, Hello Interval is 30
  Neighbor-Address Interface          Uptime    Expires
```

2.1.1.1 Vlan1 00:26:23 00:01:39

Switch#

Displayed information	Explanation
Interface (the former)	Interface name and interface IP
Owner	Multicast routing protocol of the interface
Vif	Corresponding virtual interface index to the interface
Hello Interval	The HELLO packet interval configured on the interface (in seconds)
Neighbor-Address	Neighbor address
Interface (the latter)	The neighbor interface discovered
Uptime	The up time of the neighbor since discovery
Expires	The remaining time before considering the neighbor to be invalid

19.3.4.5 debug ip pim

- **Command: debug ip pim**

Function: Enables the debugging function for displaying detailed PIM information; the "**no**" format of this command disables this debug function.

Parameters: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about PIM packets etc. is required, this debugging command can be used.

Example:

Switch # debug ip pim

00:15:45: PIM: Send v2 Hello on vlan1, holdtime 105

00:15:45: PIM: Send v2 Hello on vlan1, holdtime 105

00:15:45: PIM: Received v2 Hello on vlan1 from 2.1.1.2, holdtime 105

19.3.4.6 PIM-DM Troubleshooting Help

In configuring and using PIM-DM protocol, the PIM-DM protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use "show interface" command).
- ✧ Next, enable PIM-DM protocol on the interface (use the "ip pim dense-mode" command).
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured.

If PIM-DM problems persist after the above-mentioned procedures, please run debugging commands such as "debug ip pim", and copy the output debug information in 3 minute and send the

information to Edge-Core technical service center.

19.4 PIM-SM

19.4.1 Introduction to PIM-SM

PIM-SM (Protocol Independent Multicast，Sparse Mode) is a sparse mode multicast protocol, the mode is protocol independent. It is mainly used in large scale networks with group members relatively scattered in large ranges. In contrast to the flooding-prune method in dense mode, PIM-SM protocol assumes no hosts are receiving the multicast packets, PIM-SM routers will send multicast packets to a host only when the host explicitly request for the packets.

By setting rendezvous points (RP) and bootstrap routers, PIM-SM announces multicast information to all PIM-SM routers and builds up RP-rooted shared tree with the router join/prune information. As a result, the bandwidth occupied by data packets and control packets can be reduced, and router processing overhead can be lowered. Multicast data move along the shared tree to the network segments of the multicast group members. When the data traffic reachs a certain level, the multicast stream can be toggled to source-based shortest path tree to reduce network lag. PIM-SM is independent of specific unicast routing protocol, but uses the existing unicast routing table for RPF check.

1. How PIM-SM works

PIM-SM workflow is mainly comprised of the following parts: neighbor discovery, RP shared tree generation, multicast source registration and SPT toggle, etc. The neighbor discovery mechanism is the same as PIM-DM and is omitted here.

(1) RP shared tree (RPT) generation

When a host joins a multicast group G, the leaf route directly connected with the host learns the presence of recipient of multicast group G through IGMP packets. The router then calculates the corresponding rendezvous point (RP) for the multicast group G, and sends a join message to the upstream node in the RP direction. Each router between the leaf router and the RP will create a (*, G) entry in their forwarding table, indicating packets sent by any source to multicast group G applies to this entry. When RP receives a packet sending to multicast group G, the packet will move along the established route to reach the leaf router and the host. This completes a RP-rooted RPT.

(2) Multicast source registration.

When multicast source S sends a multicast packet to multicast group G, the PIM-SM multicast router directly connected to it will see the multicast packet as a registration packet and unicast to the appropriate RP. If multiple PIM-SM multicast routers exist in the network, the designated router (DR) is responsible for the forwarding of this multicast packet.

(3) SPT toggle

When multicast router finds the multicast packets from RP destined to G in a speed exceeding the threshold, the multicast router will send a join message to the upstream node in the source S direction and cause the toggling from RPT to SPT.

2. Pre-PIM-SM configuration work

(1) Configure candidate RP

In PIM-SM networks, multiple RPs are allowed, they are referred to as the candidate RP (C-RP).

Each C-RP is responsible for the forwarding of multicast packet destined to a certain range of addresses. Configuring multiple C-RP enables RP load balance. All C-RPs are of the same priority. On receiving BSR advertised C-RP messages, multicast routers will calculate the RP corresponding to a certain multicast group with the same algorithm.

It should be noted that one RP can service multiple multicast groups or all multicast groups. Each multicast group in any time can have only one corresponding RP, multiple associations is forbidden.

2) Configure BSR

BSR is the core of management in PIM-SM networks; it is responsible for gathering information from C-RP and broadcasting the information gathered.

Each network can have one BSR, and several Candidate-BSRs (C-BSRs). This way, once a BSR fails, another BSR will quickly take its place. BSR will be decided by the auto-election between C-BSRs.

19.4.2 PIM-SM Configuration

19.4.2.1 PIM-SM Configuration Task Sequence

1. Enable PIM-SM protocol

Basic configuration of PIM-SM routing protocol on ES4704BD series switches is quite simple: just enable PIM-SM in the appropriate interfaces.

Command	Explanation
Interface Mode	
ip pim sparse-mode **no ip pim sparse-mode**	Enable PIM-SM protocol; the "**no ip pim sparse-mode**" command disables PIM-SM protocol (required)

2. Configure PIM-SM sub-parameters

1) Configure PIM-SM interface parameters

1) Configure PIM-SM HELLO packet interval

Command	Explanation
Interface Mode	
ip pim query-interval <*query interval*> **no ip pim query-interval**	Sets interval for sending PIM-SM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

2) Configure the interface as the PIM-SM BSR border

Command	Explanation
Interface Mode	
ip pim bsr-border **no ip pim bsr-border**	Sets the interface as the PIM-SM BSR border; the "**no ip pim bsr-border**" command cancels the setting of BSR border.

2) Configure PIM-SM global parameters

1) Configure a switch as the candidate BSR.

Command	Explanation
Interface Mode	
ip pim bsr-candidate <*ifname*> [*hashlength*] [*Priority*] **no ip pim bsr-candidate**	This command is a global candidate BSR configuration command. It is used to configure information for PIM-SM candidate BSR and to contend for the BSR router with the other candidate BSRs; the "**no ip pim bsr-candidate**" command cancels the BSR configuration.

2) Configure a switch as the candidate RP.

Command	Explanation
Interface Mode	
ip pim rp-candidate <*ifname*> [group-list *access-list*] [interval *interval*] **no ip pim rp-candidate [<*ifname*>]**	This command is a global candidate RP configuration command. It is used to configure information for PIM-SM candidate RP and to contend for the RP router with the other candidate RPs; the "**no ip pim rp-candidate [<*ifname*>]**" command cancels the RP configuration.

3) Disable PIM-SM protocol

Command	Explanation
Interface Mode	
no ip pim sparse-mode	Disables PIM-SM protocol

19.4.2.2 PIM-SM Configuration Commands

- **ip pim sparse-mode**
- **ip pim bsr-border**
- **ip pim query-interval**
- **ip pim bsr-candidate**
- **ip pim rp-candidate**
- **show ip pim bsr-router**
- **show ip pim interface**
- **show ip pim mroute sm**
- **show ip pim neighbor**
- **show ip pim rp**
- **debug ip pim**
- **debug ip pim bsr**

19.4.2.2.1 ip pim sparse-mode

Command: ip pim sparse-mode
no ip pim sparse-mode

Function: Enables PIM-SM protocol on the interface; the "**no ip pim sparse-mode**" command disables PIM-SM protocol on the interface.

Parameters: N/A.

Default: PIM-SM protocol is disabled by default.

Command mode: Interface Mode

Usage Guide:

Example: Enabling PIM-SM protocol on interface vlan1.

Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip pim sparse-mode

19.4.2.2.2 ip pim bsr-border

Command: ip pim bsr-border
no ip pim bsr-border

Function: This command is the configuration command for interface BSR border. It is used to configure the border for PIM-SM area to prevent BSR message flooding outside the local PIM-SM area; the "**no ip pim bsr-border**" command cancels the BSR border configuration.

Parameters: N/A.

Default: BSR border configuration on interfaces is disabled by default.

Command mode: Interface Mode

Usage Guide: This command is the configuration commands for interface BSR border. It is used to configure the border for PIM-SM area to prevent BSR message flooding outside the local PIM-SM area. In other words, BSR messages inside the local PIM-SM area cannot be transferred from this interface to the outside; to cancel the setting of BSR border, the configuration of this command should be reverted.

Example: Enable BSR border setting on interface vlan 1.

Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip pim bsr-border

19.4.2.2.3 ip pim query-interval

Command: ip pim query-interval <*query interval*>
no ip pim query-interval

Function: Set interval for sending PIM HELLO packets in the interface; the "**no ip pim query-interval**" command restores the default setting.

Parameters: <***query interval***> is the interval for sending PIM HELLO packets, ranging from 1 to 18724s.

Default: The default interval for sending PIM HELLO is 30 seconds..

Command mode: Interface Mode

Usage Guide: The HELLO message enables PIM-DM switches to locate each other and establish the neighborhood. PIM-DM switches claim their existence by sending HELLO messages to their neighbors. If no HELLO message from a neighbor is received in a specified period, that neighbor is considered to be lost. This time setting must be no greater than the neighbor timeout time.

Example: Configuring PIM-SM HELLO interval on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim query-interval 20

19.4.2.2.4 ip pim bsr-candidate

Command: ip pim bsr-candidate <*ifname*> [*hash-mask-length*] [*priority*]

no ip pim bsr-candidate

Function: This command is a global candidate BSR configuration command. It is used to configure information for PIM-SM candidate BSR and to contend for the BSR router with the other candidate BSRs; the "**no ip pim bsr-candidate**" command cancels the BSR configuration.

Parameters: ***ifname*** is the name of the specified interface; **[*hash-mask-length*]** is the mask length of the specified hash algorithm used in RP boot selection, ranging from 0 to 32; **[*priority*]** is the BSR priority of this candidate BSR, ranging from 0 to 255, if this parameter is omitted, the priority of this candidate BSR will be defaulted to 0.

Default: The switch is not a BSR candidate router by default.

Command mode: Global Mode

Usage Guide: This command is a global candidate BSR configuration command. It is used to configure information for PIM-SM candidate BSR and to contend for the BSR router with the other candidate BSRs. The switch will be a BSR candidate router only when this command is configured.

Example: Setting the interface vlan1 as the BSR message sending interface.

Switch (Config)# ip pim bsr-candidate vlan1 30 10

19.4.2.2.5 ip pim rp-candidate

Command: ip pim rp-candidate <ifname> [group-list access-list] [interval interval]

no ip pim rp-candidate [<*ifname*>]

Function: This command is a global candidate RP configuration command. It is used to configure information for PIM-SM candidate RP and to contend for the RP router with the other candidate RPs; the "**no ip pim rp-candidate [<*ifname*>]**" command cancels the RP configuration.

Parameters: **<*ifname*>** is the name of specified interface; ***access-list*** is the number of group range list can be used as the RP in the switch, ranging from 1 to 99, if this parameter is

omitted, the router can work as the RP for all multicast groups; ***interval*** is the interval for the local candidate RP to send C-RP packets, ranging from 1 to 16383 seconds.

Default: The switch is not a BSR candidate router by default.

Command mode: Global Mode

Usage Guide: This command is a global candidate RP configuration command. It is used to configure information for PIM-SM candidate RP and to contend for the RP router with the other candidate RPs. The switch will be a RP candidate router only when this command is configured.

Example: Setting the interface vlan1 as the candidate RP announcing message sending interface.

Switch (Config)# ip pim rp-candidate vlan1 group-list 5

Switch (Config)# access-list 5 permit 239.255.2.0 0.0.0.255

19.4.3 Typical PIM-SM Scenario

As shown in the figure below, the Ethernet interfaces of SWITCHA, SWITCHB, SWITCHC and SWITCHD are added to the appropriate vlan, and PIM-SM protocol is enabled on each vlan interface.

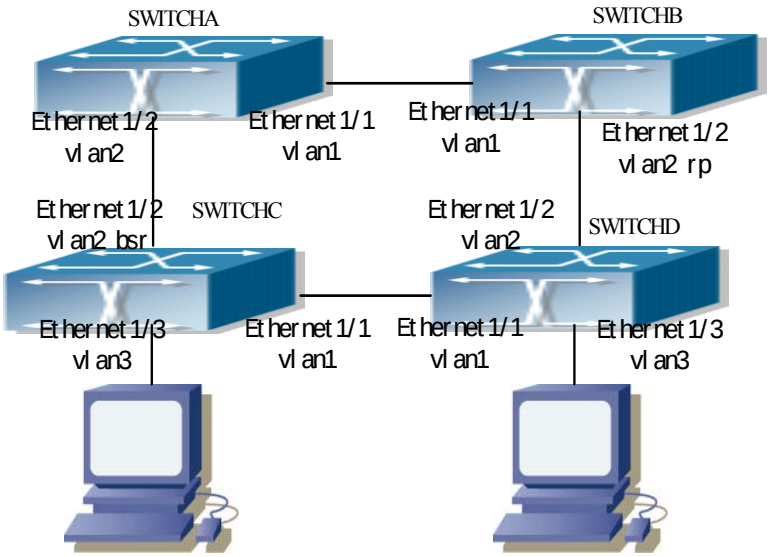


Fig 19-2 Typical PIM-SM environment

The followings are the configurations of SWITCHA, SWITCHB, SWITCHC, and SWITCHD.

(1) Configuration of SWITCHA:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)# ip pim sparse-mode

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
(2) Configuration of SWITCHB:
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)# exit
Switch (Config)# ip pim rp-candidate vlan2 group-list 5
Switch (Config)# access-list 5 permit 239.255.2.0 0.0.0.255
(3) Configuration of SWITCHC:
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode
Switch(Config-If-Vlan3)# exit
Switch (Config)# ip pim bsr-candidate vlan2 30 10
(4) Configuration of SWITCHD:
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)# ip pim sparse-mode
Switch(Config-If-Vlan1)#exit
Switch (Config)#interface vlan 2
Switch(Config-If-Vlan2)# ip pim sparse-mode
Switch(Config-If-Vlan2)#exit
Switch (Config)#interface vlan 3
Switch(Config-If-Vlan3)# ip pim sparse-mode

19.4.4 PIM-SM Troubleshooting Help

19.4.4.1 Monitor and Debug Commands

19.4.4.1.1 show ip pim bsr-router

Command: show ip pim bsr-router

Function: Displays pim bsr-router information.

Parameters: N/A.

Default: No display by default.

Command mode: Admin Mode

Example: Displaying pim bsr-router information.

Switch #show ip pim bsr-router

Switch #

PIMv2 Bootstrap information

BSR address: 192.4.1.3

Priority: 192, Hash mask length: 30

Expires : 00:02:13.

Switch #

Displayed information	Explanation
BSR address	Bsr-router address
Priority	Bsr-router priority
Hash mask length	Bsr-router hash mask length
Expires	The remaining time before considering the Bsr-router to be invalid.

19.4.4.1.2 show ip pim interface

Command: show ip pim interface [<*ifname*>]

Function: Displays information for the PIM interface.

Parameters: **<*ifname*>** is the interface name, i.e., displays PIM information of the specified interface.

Default: No display by default.

Command mode: Admin Mode

Function: Displaying PIM information of interface vlan 2.

Switch #show ip pim interface vlan2

Switch #

Interface Vlan2 : 192.3.1.2

owner is pimsm, Vif is 1, Hello Interval is 30, pim sm jp interval is (60)

Neighbor-Address Interface Uptime Expires

192.3.1.3 Vlan2 00:12:18 00:01:38

Switch #

Displayed information	Explanation
Interface (the former)	Interface name and interface IP.
owner	Multicast routing protocol of the interface.

Vif	Corresponding virtual interface index to the interface.
Hello Interval	The HELLO packet interval configured on the interface (in seconds)
jp interval	Join/prune interval.
Neighbor-Address	Neighbor address
Interface (the latter)	The neighbor interface discovered.
Uptime	The up time of the neighbor since discovery.
Expires	The remaining time before considering the neighbor to be invalid.

19.4.4.1.3 show ip pim mroute sm

Command: show ip pim mroute sm

Function: Displays the PIM-SM packet forwarding entry

Parameters: N/A.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: This command is used to display PIM-SM multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example:

```
Switch # show ip pim mroute sm
BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;
      Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;
      Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;
PIMSM Group Table, inodes 1 routes 1:
(192.1.1.1, 225.0.0.1), protos: 0x8, flags: 0x0, 00:10:18/00:03:18
  Incoming interface : Vlan1, RPF Nbr 0.0.0.0, pref 0, metric 0
  Outgoing interface list:
    (Vlan2), protos: 0x2, UpTime: 00:10:18, Exp:00:03:18
Switch #
```

Displayed information	Explanation
(192.1.1.1, 225.0.0.1)	Forwarding entry.
Incoming interface	Incoming interface, or RPF interface.
Outgoing interface list	Outgoing interface list.

19.4.4.1.4 show ip pim neighbor

Command: show ip pim neighbor [<*ifname*>]

Function: Displays information for neighbors of the PIM interface.

Parameters: <***ifname***> is the interface name, i.e., displays PIM neighbor information of the

specified interface.

Default: No display by default.

Command mode: Admin Mode

Usage Guide: If no interface name is specified, then neighbor information for all interfaces will be displayed.

Example: Displaying neighbor information for all interfaces (do not specify the interface name)

Switch # **show ip pim neighbor**

Neighbor-Address	Interface	ifIndex	Uptime	Expires	DR-state
192.3.1.3	Vlan1	28	00:11:39	00:01:16	DR
192.2.1.1	Vlan2	31	00:11:39	00:01:16	/
192.4.1.4	Vlan4	33	00:11:39	00:01:44	DR
192.4.1.3	Vlan4	33	00:11:39	00:01:17	/

Switch #

Displayed information	Explanation
Neighbor-Address	Neighbor address
Interface	The neighbor interface discovered
ifIndex	Interface index number
Uptime	The up time of the neighbor since discovery
Expires	The remaining time before considering the neighbor to be invalid
DR-state	Whether the neighbor is a DR

19.4.4.1.5 show ip pim rp

Command: show ip pim rp [**mapping** | ***group-address***]

Function: Displays PIM RP related information

Parameters: mapping displays the group address and RP association.

group-address is the group address.

Default: No display by default.

Command mode: Admin Mode

Function: Displaying the RP information for PIM area 226.1.1.1.

Switch #show ip pim rp 226.1.1.1

RP Address for this group is: 192.2.1.1

Displayed information	Explanation
RP Address	RP address of the group

19.4.4.1.6 debug ip pim

- **Command: debug ip pim**

Function: Enables the debugging function for displaying detailed PIM information; the "**no**" format

of this command disables this debug function.

Parameters: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about PIM packets etc. is required, this debugging command can be used.

Example:

Switch # debug ip pim

PIM debug is on

00:17:52: PIM: Received v2 Join/Prune on Vlan2 from 192.3.1.3 to 192.3.1.2

00:17:52: PIM: Receive Join-list: (192.1.1.1/32, 225.0.0.1/32), S-bit set

00:17:54: PIM: Received v2 Hello on Vlan4 from 192.4.1.4, holdtime 105

00:17:57: PIM: Received v2 Hello on vlan3 from 192.2.1.1, holdtime 105

00:17:57: PIM: Received v2 Hello on Vlan2 from 192.3.1.3, holdtime 105

00:17:58: PIM: Received v2 Hello on Vlan4 from 192.4.1.3, holdtime 105

00:18:21: PIM: Send v2 Hello on vlan2, holdtime 105

00:18:21: PIM: Send v2 Hello on vlan4, holdtime 105

00:18:21: PIM: Send v2 Hello on vlan3, holdtime 105

00:18:21: PIM: Send v2 Hello on Vlan4, holdtime 105

00:18:21: PIM: Send v2 Hello on Vlan2, holdtime 105

19.4.4.1.7 debug ip pim bsr

Command: debug ip pim bsr

Function: Enables the PIM candidate RP/BSR information debug function; the "**no**" format of the command disables this debug function.

Parameters: N/A.

Default: Disabled

Command mode: Admin Mode

Usage Guide: If detailed information about PIM candidate RP/BSR packets etc. is required, this debugging command can be used.

Example:

Switch # debug ip pim bsr

PIM BSR debug is on

00:16:23: PIM: Received v2 BSR on Vlan4 from 192.4.1.3

00:16:23: PIM: Receive BSR fragtag 6879, hmlen: 30, pri: 192

00:16:23: PIM: Receive BSR Group (225.0.0.1, 0.0.0.0): rpcount: 1, fragcount: 1

00:16:23: PIM: C-RP 192.2.1.1, holdtime 130, C-RP pri 192

00:16:23: PIM: Transmit the BSR message on Vlan2

00:16:23: PIM: Transmit the BSR message on vlan4

00:16:23: PIM: Transmit the BSR message on vlan3
00:16:23: PIM: Transmit the BSR message on vlan2

19.4.4.2 PIM-SM Troubleshooting

In configuring and using PIM-SM protocol, the PIM-SM protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use "show interface" command).
- ✧ Multicast protocols use unicast routes to perform RPF checks, for this reason, the unicast route correctness must be ensured.
- ✧ PIM-SM protocol requires the support of RP and BSR. So "**show ip pim bsr-router**" command should be run first for BRS information, if no BSR exists, then the unicast route to BSR should be checked.
- ✧ Use the "**show ip pim rp**" command to verify RP information is correct. If no RP information is displayed, the unicast route should be checked, too.

If PIM-SM problems persist after the above-mentioned procedures, please run debugging commands such as "debug ip pim" / "debug ip pim bsr", and copy the output debug information in 3 minute and send the information to Edge-Core technical service center.

19.5 DVMRP

19.5.1 Introduction to DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is a dense mode multicast routing protocol. It employs a RIP like route exchange mechanism to establish a forwarding broadcast tree for each source, then a truncated broadcast tree (short path tree to the source) will be created by dynamic pruning/grafting. Reverse path forwarding (RPF) is used to decide whether multicast packet should be forwarded to the downstream nodes.

The following are some important DVMRP features:

1. The route exchange process determining RPF information is based on distance vectors (in the way similar to RIP)
2. Route exchange occurs periodically (every 60 seconds by default)
3. Maximum TTL = 32 hops (rather than the 16 hops in RIP)
4. Mask included in route update packet, CIDR supported.

Comparing to unicast routing, the multicast routing is a reversed route (i.e., interest is in where the packet comes from instead of where it is going to). This is why the route table information in DVMRP is used to determine whether the incoming multicast packet is arriving at the correct interface. The packet is discarded if the interface is not correct to prevent multicast loop.

The test to determine whether a packet is arriving at the correct interface is called RPF check. When a multicast packet arrives at an interface, the DVMRP route table will be checked to decide the reverse path to the source network. If the interface at which the packet arrives is the interface to

send unicast information to the source, then the RPF check is success and the packet is forwarded from all down stream interfaces. Otherwise, there may be something wrong, and the multicast packet is discarded.

Since not all switches support multicast, DVMRP provide support for tunneling multicast information. Tunneling is a method used between DVMRP switches separated by non-multicast routing switch(es). A tunnel acts as the virtual network between two DVMRP switches. The multicast packet is encapsulated in a unicast packet and destined to a multicast-enabled switch. DVMRP treats tunneling interface the same way as common physical interfaces.

If two or more switches are connected to a multi-egress network, multiple copies of a packet may be sent to the subnet. Therefore, a specific forwarder must be specified. DVMRP fulfills this by routing switch mechanism. When two switches in a multi-egress network are exchanging routing information, they know the route metric for each other to get to the source network, and the switch has the smallest metric to the source network becomes the designated forwarder of that subnet; if the metrics are same, the one with lower IP address rules.

When DVMRP is enabled on an interface of the switch, probe messages are multicasted to the other DVMRP switches to discover the neighbors and their capabilities. If no probe messages from a neighbor is received before the neighbor times out, it is regarded as lost.

In DVMRP, source network route selection information is exchanged in the same basic way like the RIP. That is to say, route advertisements are sent between DVMRP neighbors periodically (every 60 seconds by default). The routing information in the DVMRP route selection table is used to establish the source distribution tree, which can be used to determine which neighbor can reach the source sending multicast information. Interfaces leading to this neighbor are referred to as the upstream interface. Routing report packet contains source network and the hops for assessing route metrics.

To forward properly, each DVMRP switch need to know in what specific interface the multicast information should be received for the downstream switches. When a multicast packet from a specific source is received, a DVMRP switch will first broadcast the multicast packet in all downstream interfaces (interfaces in which other DVMRP switches have indicated dependency). On receiving a prune message from a downstream switch, that switch will be pruned. The DVMRP switch informs an upstream switch for a certain source by poison reverse: “I am your downstream.” The DVMRP switch fulfills the poison reverse by adding infinite (32) to the route metric of a certain source broadcasted by it in replying its upstream switches. Hence correct metric value can be 1 to (2 x infinite (32) -1), or 1 to 63. 1 to 31 indicates a reachable source network, 32 indicates an unreachable source, 33 to 63 indicates the switch generating the report message depend on upstream switches to receive multicast information from certain source.

19.5.2 DVMRP configuration

19.5.2.1 Configuration Task Sequence

1. Enable DVMRP (required)
2. Configure connectivity with CISCO routers/switches (optional)
3. Configure DVMRP sub-parameters (optional)

(1) Configuring DVMRP interface parameters.

a. Configure metric value for DVMRP report packet

b. Configuring DVMRP neighbor timeout time

(2) Configuring DVMRP global parameters.

a. Configure retransmission interval for graft packets in DVMRP
b. Configure transmission interval of probe packets in DVMRP
c. Configure transmission interval of report packets in DVMRP
d. Configuring DVMRP route timeout time

4. Configure DVMRP tunneling
5. Disable DVMRP

1. Enable DVMRP

Basic configuration of DVMRP routing protocol on ES4704BD series switches is quite simple: just enable DVMRP in the appropriate interfaces.

Command	Explanation
Interface Mode	
[no] ip dvmrp enable	Enable DVMRP; the "**no ip dvmrp enable**" command disables DVMRP (required)

2. Configure connectivity with CISCO routers/switches

CISCO does not really implemented DVMRP, but provides connectivity with DVMRP. As CISCO routers/switches send report packet but not probe packets, neighbor timeout issue should be addressed in establish connectivity with CISCO routers/switches. The following command makes a ES4704BD switch to decide the timeout of a neighbor by report packet intervals.

Command	Explanation
Interface Mode	
[no] ip dvmrp cisco-compatible <*A.B.C.D*>	Enables connectivity with CISCO neighbor A, B, C, D; the "**no ip dvmrp cisco-compatible**" command disables connectivity with CISCO neighbors.

3. Configure DVMRP sub-parameters

(1) Configuring DVMRP interface parameters.

a. Configure metric value for DVMRP report packet
b. Configure DVMRP neighbor timeout time

Command	Explanation
Interface Mode	
ip dvmrp metric <*metric_val*> **no ip dvmrp metric**	Sets interval for sending DVMRP report packets in the interface; the "**no ip dvmrp metric**" command restores the default setting.
ip dvmrp nbr-timeout <*time_val* > **no ip dvmrp nbr-timeout**	Sets timeout interval for DVMRP neighbors in the interface; the "**no ip dvmrp nbr-timeout**" command restores the default setting.

(2) Configuring DVMRP global parameters.

a. Configure transmission interval of graft packets in DVMRP
b. Configure transmission interval of probe packets in DVMRP

c. Configure transmission interval of report packets in DVMRP

Command	Explanation
Global Mode	
ip dvmrp graft-interval <*time_val*> **no ip dvmrp graft-interval**	Sets the interval for sending DVMRP graft messages; the "**no ip dvmrp graft-interval**" command restores the default setting.
ip dvmrp probe-interval <*time_val*> **no ip dvmrp probe -interval**	Sets the interval for sending DVMRP probe messages; the "**no ip dvmrp probe interval**" command restores the default setting.
ip dvmrp report-interval <*time_val*> **no ip dvmrp report-interval**	Sets the interval for sending DVMRP report messages; the "**no ip dvmrp report interval**" command restores the default setting.

d. Configuring DVMRP route timeout time

Command	Explanation
Global Mode	
ip dvmrp route-timeout <*time_val*> **no ip dvmrp route-timeout**	Sets timeout interval for DVMRP routes; the "**no ip dvmrp route-timeout**" command restores the default setting.

4. Configure DVMRP tunneling

Command	Explanation
Interface Mode	
ip dvmrp tunnel <A.B.C.D> [metric <metric_val>] **no ip dvmrp tunnel <*A.B.C.D*>**	Configures tunneling to neighbor A, B, C, D; the "**no ip dvmrp tunnel**" command removes the tunnel to neighbor A, B, C, D.

5. Disable DVMRP

Command	Explanation
Interface Mode	
no ip dvmrp enable	Disables DVMRP

19.5.2.2 DVMRP Configuration Commands

- **ip dvmrp cisco-compatible**
- **ip dvmrp enable**
- **ip dvmrp graft-interval**
- **ip dvmrp metric**
- **ip dvmrp nbr-timeout**
- **ip dvmrp probe-interval**
- **ip dvmrp report-interval**
- **ip dvmrp route-timeout**

- **ip dvmrp tunnel**
- **show ip dvmrp mroute**
- **show ip dvmrp neighbor**
- **show ip dvmrp route**
- **show ip dvmrp tunnel**
- **debug ip dvmrp detail**
- **debug ip dvmrp pruning**

19.5.2.2.1 ip dvmrp cisco-compatible

Command: ip dvmrp cisco-compatible <*A.B.C.D*>

no ip dvmrp cisco-compatible <*A.B.C.D*>

Function: Enables connectivity with CISCO neighbor A, B, C, D; the "**no ip dvmrp cisco-compatible**" command disables connectivity with CISCO neighbors.

Parameters: <*A.B.C.D*> are the Neighboring IP addresses

Default: The connectivity with CISCO neighbors is disabled by default.

Command mode: Interface Mode

Usage Guide: CISCO does not really implement DVMRP, but provides connectivity with DVMRP. As CISCO routers/switches send report packets but not probe packets, neighbor timeout issues should be addressed in establish connectivity with CISCO routers/switches. Configuration of this command enables the switch to tell neighbor timeout by report packet intervals (if no report message format a CISCO neighbor is received in an interval three times of the report interval, that neighbor is considered to be timeout.

Example: Enabling connectivity with CISCO neighbor 1.1.1.1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp cisco-compatible 1.1.1.1

19.5.2.2.2 ip dvmrp enable

Command: ip dvmrp enable

no ip dvmrp enable

Function: Enables DVMRP on the interface; the "**no ip dvmrp enable**" command disables DVMRP on the interface.

Parameters: N/A.

Default: DVMRP is disabled by default.

Command mode: Interface Mode

Usage Guide:

Example: Enabling DVMRP on interface vlan1.

Switch (Config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp enable

19.5.2.2.3 ip dvmrp graft-interval

Command: ip dvmrp graft-interval <*time_val*>
no ip dvmrp graft-interval

Function: Sets the interval for sending DVMRP graft messages; the "**no ip dvmrp graft-interval**" command restores the default setting.

Parameters: <***time_val***> is the interval for sending DVMRP graft packets, ranging from 5 to 3600 seconds.

Parameters: The default interval for sending DVMRP graft messages is 5 seconds.

Command mode: Global Mode

Usage Guide: If a new receiver joins that interface when an interface is in the pruned state, the interface will send a graft message to the upstream; if no graft ACK message from the upstream is received, it will keep sending graft message to the upstream at regular interval until an appropriate graft ACK is received.

Example: Setting the interval for sending DVMRP graft messages to 10 seconds.

Switch (Config)#ip dvmrp graft-interval 10

19.5.2.2.4 ip dvmrp metric

Command: ip dvmrp metric <*metric_val*>
no ip dvmrp metric

Function: Sets the interval for sending DVMRP report packets in the interface; the "**no ip dvmrp metric**" command restores the default setting.

Parameters: < *metric_val*> is the route metric value, ranging from 1 to 32.

Default: The default tag value is 1.

Command mode: Interface Mode

Usage Guide: The routing information in a DVMRP report packet includes a list of source network addresses and metrics. When DVMRP report packet metric is configured on the interface, all route entries received on that interface will be added the interface metric value configured to form a new metric value. The metric value is used for poison reverse calculation to determine upstream/downstream conditions. If a route metric in the local switch is greater than 32 or equal to 32, then this route is unreachable. If after calculation, the switch confirms itself in the downstream of a route, then a report message containing that route will be sent to the upstream, with the metric added by 32 to indicate the downstream position.

Example: Configuring the DVMRP report packet metric to 2 on the interface.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp metric 2

19.5.2.2.5 ip dvmrp nbr-timeout

Command: ip dvmrp nbr-timeout <*time_val*>
no ip dvmrp nbr-timeout

Function: Sets the timeout interval for DVMRP neighbors in the interface; the "**no ip dvmrp nbr-timeout**" command restores the default setting.

Parameters: < *time_val*> is the time to timeout a neighbor, the valid range is 20 to 8000 seconds.

Default: The default neighbor timeout setting is 35 seconds.

Command mode: Interface Mode

Usage Guide: When neighborhood established in DVMRP, a neighbor is considered nonsexist if no probe message from that neighbor is received in the neighbor timeout interval, and the neighborhood is terminated. Neighbor timeout interval must be greater than the interval for sending probe messages.

Example: Configuring the DVMRP neighbor timeout interval for the interface as 30 seconds.

Switch (Config)#interface vlan 1

Switch(Config-If-vlan1)#ip dvmrp nbr-timeout 30

19.5.2.2.6 ip dvmrp probe-interval

Command: ip dvmrp probe-interval <*time_val*>

no ip dvmrp probe-interval

Function: Sets the interval for sending DVMRP probe messages; the "**no ip dvmrp probe interval**" command restores the default setting.

Parameters: <***time_val***> is the interval for sending DVMRP probe packets, ranging from 5 to 30 seconds..

Default: The default interval for sending DVMRP probe messages is 10 seconds.

Command mode: Global Mode

Usage Guide: The probe message enables DVMRP switches to locate each other and establish the neighborhood, and to learn the capability of each other. DVMRP switches claim their existence by sending probe message to their neighbors. If no probe message from a neighbor is received in a specified period, that neighbor is considered to be lost. This time must be no greater than the neighbor timeout time.

Example: Setting the interval for sending DVMRP probe messages to 20 seconds..

Switch (Config)#ip dvmrp probe-interval 20

19.5.2.2.7 ip dvmrp report-interval

Command: ip dvmrp report-interval <*time_val*>

no ip dvmrp report-interval

Function: Sets the interval for sending DVMRP report messages; the "**no ip dvmrp report-interval**" command restores the default setting.

Parameters: <***time_val***> is the interval for sending DVMRP report packets, ranging from 10 to 2000 seconds.

Default: The default interval for sending DVMRP report messages is 60 seconds.

Command mode: Global Mode

Usage Guide: DVMRP route information is exchanged in the way similar to that in RIP, i.e., in the report messages between DVMRP neighbors periodically. If no updating report message for a route from the neighbor of the route is received in the specified interval, then the route is considered to be invalid. This interval configured must be no greater than the timeout interval for the route.

Example: Setting the interval for sending DVMRP route report messages to 100 seconds.

Switch (Config)#ip dvmrp report-interval 100

19.5.2.2.8 ip dvmrp route-timeout

Command: ip dvmrp route-timeout <time_val>

no ip dvmrp route-timeout

Function: Sets timeout interval for a DVMRP route; the "**no ip dvmrp route-timeout**" command restores the default setting.

Parameters: < *time_val*> is the time to timeout a route, the valid range is 20 to 1400 seconds..

Default: The default timeout setting for DVMRP routes is 140 seconds.

Command mode: Global Mode

Usage Guide: If no updating report message for a route from the neighbor of the route is received in the specified interval, then the route is considered to be invalid. This timeout interval must be greater than that for sending report messages.

Example: Configuring the DVMRP route timeout interval to 100 seconds..

Switch (Config)#ip dvmrp route-timeout 100

19.5.2.2.9 ip dvmrp tunnel

Command: ip dvmrp tunnel <*A.B.C.D*> [metric <*metric_val*>]

no ip dvmrp tunnel <*A.B.C.D*>

Function: Configures tunneling to neighbor A, B, C, D; the "**no ip dvmrp tunnel**" command removes the tunnel to neighbor A, B, C, D.

Parameters: < *A.B.C.D*> is the IP addresses of remote neighbors; **<*metric_val*>** is the metric value for the tunneling interface, ranging from 1 to 32.

Default: DVMRP tunneling is disabled by default, the default value for **<*metric_val*>** is 1.

Command mode: Interface Mode

Usage Guide: Since not all switches support multicast, DVMRP provides support for tunneling multicast information. Tunneling is a method used between DVMRP switches separated by non-multicast routing switch(es). The tunnel acts as the virtual network between two DVMRP switches. The multicast packet is encapsulated in a unicast packet and destined to a multicast-enabled switch. DVMRP treats the tunneling interface the same way as common physical interfaces.

Example: Configuring a DVMRP tunnel on Ethernet interface vlan1 to the remote neighbor 1.1.1.1.

Switch(Config-If-Vlan1)#ip dvmrp tunnel 1.1.1.1 metric 10

19.5.3 Typical DVMRP Scenario

As shown in the figure below, the Ethernet interfaces of SwitchA and SwitchB are added to the appropriate vlan, and DVMRP protocol is enabled on each vlan interface.

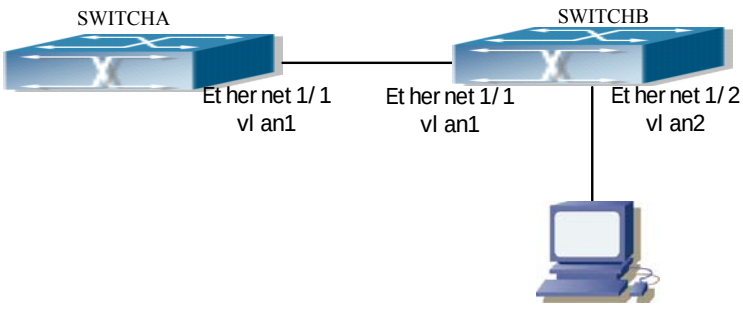


Fig 19-3 DVMRP network topology

The followings are the configurations of SwitchA and SwitchB.

(1) Configuration of SWITCHA:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp enable

(2) Configuration of SWITCHB:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip dvmrp enable

Switch(Config-If-Vlan1)#exit

Switch (Config)#interface vlan 2

Switch(Config-If-Vlan2)# ip dvmrp enable

19.5.4 DVMRP Troubleshooting Help

1. Monitor and debug commands
2. DVMRP troubleshooting help

19.5.4.1 Monitor and Debug Commands

19.5.4.1.1 show ip dvmrp mroute

Command: show ip dvmrp mroute

Function: Displays the DVMRP packet forwarding entries..

Parameters: N/A.

Default: Not displayed.

Command mode: Admin Mode

Usage Guide: This command is used to display DVMRP multicast forwarding entries, or the forwarding entries in the system FIB table for forwarding multicast packets.

Example:

Switch# show ip dvmrp mroute

BIT Proto: DVMRP 0x2, PIM 0x8, PIMSM 0x10, PIMDM 0x20;

Flags: RPT 0x1, WC 0x2, SPT 0x4, NEG CACHE 0x8, JOIN SUPP 0x10;

Downstream: IGMP 0x1, NBR 0x2, WC 0x4, RP 0x8, STATIC 0x10;

DVMRP Multicast Routing Table, inodes 1 routes 1:

(192.168.1.0, 224.1.1.1), protos: 0x2, flags: 0x0

Incoming interface : Vlan1, RPF Nbr 0.0.0.0, pref 0, metric 1

Outgoing interface list:

(Vlan2), protos: 0x2

Upstream prune interface list:

Downstream prune interface list:

Displayed information	Explanation
(192.168.1.0, 224.1.1.1)	Forwarding entry
Incoming interface	Incoming interface, or RPF interface
Outgoing interface list	Outgoing interface list
Upstream prune interface list	Upstream prune interface list
Downstream prune interface list	Downstream prune interface list

19.5.4.1.2 show ip dvmrp neighbor

Command: show ip dvmrp neighbor [<*ifname*>]

Function: Displays information for DVMRP neighbors.

Parameters: **<*ifname*>** is the interface name, i.e., displays neighbor information of the specified interface.

Default: Not displayed.

Command mode: Admin Mode

Example: Displays neighbor information of Ethernet interface vlan1.

Switch #show ip dvmrp neighbor vlan1

Switch #

Neighbor-Address	Interface	Uptime	Expires
192.168.1.22	Vlan1	00:02:22	00:00:28

Switch #

Displayed information	Explanation
Neighbor-Address	Neighbor address
Interface	The interface on which the neighbor is discovered
Uptime	The up time of the neighbor since discovery.

Expires	The remaining time before considering the neighbor to be invalid

19.5.4.1.3 show ip dvmrp route

Command: show ip dvmrp route

Function: Displays DVMRP routing information.

Parameters: N/A.

Default: Not displayed.

Command mode: Admin Mode

Usage Guide: This command is used to display DVMRP route table entries; DVMRP maintains separated unicast route tables for RPF check.

Example: Displaying DVMRP routing information.

Switch #show ip dvmrp route

Switch #

Destination/Mask	Nexthop	Interface	Gateway	Metric	state
192.168.1.0/24	192.168.1.11	Vlan1	No-Gateway	1	active

Switch #

Displayed information	Explanation
Destination/Mask	Target network segment or address and mask
Nexthop	Next hop address
Interface	The interface on which the route is discovered
Gateway	Gateway address
Metric	Route metric value
state	Route state (active, hold, etc)

19.5.4.1.4 show ip dvmrp tunnel

Command: show ip dvmrp tunnel [<*ifname*>]

Function: Displays information for a DVMRP tunnel.

Parameters: <***ifname***> is the interface name, i.e., display the tunnel information of the specified interface.

Default: Not displayed.

Command mode: Admin Mode

Example: Displaying tunneling configuration information of Ethernet interface vlan1.

Switch #show ip dvmrp tunnel vlan1

Name: dvmrp2, Index: 7, State:1195, Parent: 3, Localaddr: 192.168.1.11, Remote:

1.1.1.1

Switch #

Displayed information	Explanation
Name	Tunnel interface name (auto-generated by the system)
Index	Tunnel interface index number
State	Tunnel interface status
Parent	The index number of the parent interface for the tunnel interface
Localaddr	Local address of the tunnel interface
Remote	Remote end address of the tunnel

19.5.4.1.5 debug ip dvmrp detail

Command: debug ip dvmrp detail

Function: Enables the debug function for displaying detailed DVMRP information; the "**no**" format of this command disables this debug function.

Parameters: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If detailed information about DVMRP packets (except prune and graft) is required, this debug command can be used.

Example:

Switch#debug ip dvmrp detail
DVMRP detail debug is on
Switch#01:18:09:35: DVMRP: Received probe on vlan1 from 192.168.1.22
01:18:09:35: DVMRP: probe Vers: majorv 3, minorv 255
01:18:09:35: DVMRP: probe flags: PG
01:18:09:35: DVMRP: probe genid: 0x48
01:18:09:35: DVMRP: probe nbrs: 192.168.1.11
01:18:09:40: DVMRP: Send probe on vlan1 to 224.0.0.4, len 16
01:18:09:40: DVMRP: probe Vers: majorv 3, minorv 255
01:18:09:40: DVMRP: probe flags: PG
01:18:09:40: DVMRP: probe genid: 0x24c57
01:18:09:40: DVMRP: probe nbrs: 192.168.1.22
01:18:09:40: DVMRP: Send probe on dvmrp2 to 224.0.0.4, len 12
01:18:09:40: DVMRP: probe Vers: majorv 3, minorv 255
01:18:09:40: DVMRP: probe flags: PG
01:18:09:40: DVMRP: probe genid: 0x24f29

19.5.4.1.6 debug ip dvmrp pruning

Command: debug ip dvmrp pruning

no debug ip dvmrp pruning

Function: Enables the debug function for displaying DVMRP prune/graft information; the "**debug**

ip dvmrp pruning" command disables this debug function.

Parameters: N/A.

Default: Debug is disabled by default.

Command mode: Admin Mode

Usage Guide: If detailed DVMRP prune/graft information is required, this debug command can be used.

Example:

Switch#debug ip dvmrp pruning

DVMRP pruning debug is on

02:22:20:26: DVMRP: Received prune on vlan2 from 105.1.1.2, len 20

02:22:20:26: DVMRP: Prune Vers: majorv 3, minorv 255

02:22:20:26: DVMRP: Prune source 192.168.1.105, group 224.1.1.1

02:22:20:40: DVMRP: Received graft on vlan1 from 105.1.1.2, len 16

02:22:20:40: DVMRP: Graft Vers: majorv 3, minorv 255

02:22:20:40: DVMRP: Graft source 192.168.1.105, group 224.1.1.1

02:22:20:40: DVMRP: Send graft-ACK on vlan1 to 105.1.1.2, len 16

02:22:20:40: DVMRP: Graft-Ack Vers: majorv 3, minorv 255

02:22:20:40: DVMRP: Graft-ACK source 192.168.1.105, group 224.1.1.1

19.5.4.2 DVMRP Troubleshooting

In configuring and using DVMRP protocol, the DVMRP protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use "show interface" command).
- ✧ Ensure the interface has an IP address properly configured (use "ip address" command).
- ✧ Next, enable DVMRP on the interface (use the "ip dvmrp enable" command).
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured. (DVMRP uses its own unicast route table, use the "show ip dvmrp route" command to view that table.)
- ✧ If connectivity with CISCO is required, make sure the CISCO connex command is configured (use "ip dvmrp cisco-compatible" command)

If DVMRP problems persist after the abovementioned procedures, please run debug commands like "debug ip dvmrp detail/pruning", and copy the debug information in 3 minute and send the information to Edge-Core technical service center.

19.6 IGMP

19.6.1 Introduction to IGMP

IGMP (Internet Group Management Protocol) is a TCP/IP protocol responsible for IP multicast member management. It is used to establish and maintain multicast group membership between IP hosts and direct neighbor multicast switches. IGMP does not include the populating and maintenance of membership between multicast switches, which is covered by multicast routing protocols. All hosts participate in multicast must implement IGMP.

Hosts participate in IP multicast can join/quit multicast groups at any position, any time, and of any number. The multicast switches do not save all host memberships, which is also impractical. They just obtain information about whether receivers of a multicast group (group member) exist in network segments connecting to its interfaces. As to the hosts, they only need to keep the information about the multicast groups joined.

IGMP is asymmetric for hosts and switches: The hosts respond IGMP query packets sent by the multicast switches, i.e., respond with membership report packets. The switches send membership query packets in regular interval, and decide whether hosts of their subnet join some group or not; on receiving quit group reports from the hosts, they send query of associated group (IGMP v2) to determine whether there are members in a certain group.

There are so far three versions of IGMP: IGMP v1 (define in RFC1112), IGMP v2 (defined in RFC2236) and IGMP v3. Version 2 is the most widely used version at present.

Major improvements of IGMP v2 from v1 include:

1. Election mechanism for multicast switches in shared network segments.

A shared network segment is a segment with several multicast switches. In this case, since all switches running IGMP in the segment can receive membership report messages, only one switch is needed to send membership query messages. Therefore, there should be a switch election mechanism to determine the switch acting as the querier. In IGMP v1, the selection of querier is determined by multicast routing protocols; IGMP v2 improves this feature and specifies the multicast switch of the lowest IP address to be the querieer.

2. Quit group mechanism added in IGMP v2

In IGMP v1, the hosts quits the multicast without giving any message to any multicast switch. And multicast switches discover this by multicast group response timeout. In version2, if a host decides to quit a multicast group, and it is the host responding to the latest membership query message, it will send a quit-group message.

3. Specific group query added in IGMP v2

In IGMP v1, the query of multicast switch aims for all multicast groups in that segment. This query is called the universal group query. In IGMP v2, specific group query is introduced in addition to the universal group query. The destination IP address of such query packet is the IP address of the specified multicast group, the area part in the packet of the group address is the IP address of the specified multicast group, too. Thus response packets from the hosts of the other multicast groups can be avoided.

4. Maximum response time field added in IGMP v2

IGMP v2 has a field for maximum response time added, so that hosts response time for group query packets can be adjusted dynamically.

19.6.2 IGMP configuration

19.6.2.1 Configuration Task Sequence

1、 Enable IGMP (required)

2、 Configure IGMP sub-parameters (optional)

(1) Configure IGMP group parameters.

a. Configuring IGMP group filtering criteria

b. Configure IGMP groups

c. Configure static IGMP groups

(2) Configure IGMP query parameters.

a. Configure transmission interval of query packets in IGMP

b. Configure maximum response time for IGMP queries

c. Configure timeout setting for IGMP queries

(3) Configure IGMP version

3、 Disable IGMP

1. Enable IGMP

There is no special command for enabling IGMP in ES4704BD layer 3 switches, the IGMP automatically enables when any multicast protocol is enabled on the respective interface.

Command	Explanation
Interface Mode	
ip dvmrp enable | ip pim dense-mode | ip pim sparse-mode	Enables IGMP protocol; the "**no pim sparse-mode**" command disables IGMP protocol (required)

2. Configure IGMP sub-parameters

(1) Configure IGMP group parameters.

a. Configure IGMP group filtering criteria

b. Configure IGMP groups

c. Configure static IGMP groups

Command	Explanation
Interface Mode	
ip igmp access-group {<*acl_num* | *acl_name*>} **no ip igmp access-group**	Sets the filter criteria for IGMP group on the interface; the "**no ip igmp access-group**" command cancels the filter criteria.
ip igmp join-group <*A.B.C.D* > **no ip igmp join-group <*A.B.C.D* >**	Joins the interface to an IGMP group; the "**no ip igmp join-group**" command cancels the join.

ip igmp static-group <*A.B.C.D* > **no ip igmp static -group <*A.B.C.D* >**	Joins the interface to a static IGMP group; the "**no ip igmp static -group**" command cancels the join.

(2) Configure IGMP query parameters.

a. Configure transmission interval of query packets in IGMP

b. Configure maximum response time for IGMP queries

c. Configure timeout setting for IGMP queries

Command	Explanation
Interface Mode	
ip igmp query-interval <*time_val*> **no ip igmp query-interval**	Sets the interval for sending IGMP query messages; the "**no ip IGMP query interval**" command restores the default setting.
ip igmp query-max-response-time <*time_val*> **no ip igmp query-max-response-time**	Sets the maximum time for an interface to response to an IGMP query; the "**no ip igmp query-max-response-time**" command restores the default setting.
ip igmrp query-timeout <*time_val*> **no ip igmp query-timeout**	Sets the timeout interval for an interface to response to an IGMP query; the "**no ip igmp query-timeout**" command restores the default setting.

(3) Configure IGMP version

Command	Explanation
Interface Mode	
ip igmp version <*version*> **no ip igmp version**	Configures the IGMP version of the interface; the "**no ip igmp version**" command restores the default setting.

3. Disable IGMP

Command	Explanation
Interface Mode	
no ip dvmrp enable | no ip pim dense-mode | no ip pim sparse-mode	Disables IGMP

19.6.2.2 IGMP Configuration Commands

- **ip igmp access-group**
- **ip igmp join-group**
- **ip igmp query-interval**
- **ip igmp query-max-response-time**
- **ip igmp query-timeout**

- **ip igmp static-group**
- **ip igmp version**
- **show ip igmp groups**
- **show ip igmp interface**
- **debug ip igmp event**
- **debug ip igmp packet**

19.6.2.2.1 ip igmp access-group

Command: ip igmp access-group {<*acl_num* | *acl_name*>}
no ip igmp access-group

Function: Sets the filter criteria for IGMP group on the interface; the "**no ip igmp access-group**" command cancels the filter criteria.

Parameters: {<*acl_num* | *acl_name*>} is the sequence number of name of the access list, where the range of ***acl_num*** is 1 to 99.

Default: No filter criteria is set by default

Command mode: Interface Mode

Usage Guide: This command can be issued to filter the groups on the interface to allow or deny the participant of some groups.

Example: Specify interface vlan1 to permit 224.1.1.1 and deny 224.1.1.2.

Switch (Config)#access-list 1 permit 224.1.1.1 0.0.0.0
Switch (Config)#access-list 1 deny 224.1.1.2 0.0.0.0
Switch (Config)#interface vlan 1
Switch(Config-If-Vlan1)#ip igmp access-group 1

19.6.2.2.2 ip igmp join-group

Command: ip igmp join-group <*A.B.C.D* >
no ip igmp join-group <*A.B.C.D* >

Function: Joins the interface to an IGMP group; the "**no ip igmp join-group**" command cancels the join.

Parameters: <*A.B.C.D*> are the IP addresses for multicast groups.

Default: not joined to groups.

Command mode: Interface Mode

Usage Guide: When a switch is used as a host, this command is used to any the host to a group. Suppose the local interface is to be added to group 224.1.1.1, then the switch will send a IGMP member report containing group 224.1.1.1 on receiving IGMP group query from the other switches. Note the difference between this command and the "**ip igmp static-group**" command.

Example: Specifying interface vlan1 to join group 224.1.1.1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp join-group 224.1.1.1

19.6.2.2.3 ip igmp query-interval

Command: ip igmp query-interval <*time_val*>
no ip igmp query-interval

Function: Sets the interval for sending IGMP query messages; the "**no ip IGMP query interval**" command restores the default setting.

Parameters: <***time_val***> is the interval for sending IGMP query packets, ranging from 1 to 65535 seconds.

Default: The default interval for sending IGMP query messages is 125 seconds.

Command mode: Interface Mode

Usage Guide: When a multicast protocol is enabled on an interface, IGMP query message will be sent at regular interval from this interface. This command is also used to configure the query period.

Example: Setting the interval for sending IGMP query messages to 10 seconds..

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-interval 10

19.6.2.2.4 ip igmp query-max-response-time

Command: ip igmp query-max-response-time <*time_val*>
no ip igmp query- max-response-time

Function: Sets the maximum time for an interface to response to an IGMP query; the "**no ip igmp query-max-response-time**" command restores the default setting.

Parameters: <***time_val***> is the maximum interface response time for IGMP queries, ranging from 1 to 25 seconds.

Default: The default value is 10 seconds.

Command mode: Interface Mode

Usage Guide: On receiving a query message from the switch, the host will set a counter for each multicast group it belongs to, the counter value is random from 0 to the maximum response time. When the value of any counter decreases to 0, the host will send the member report message for the multicast group. Setting the maximum response time sensibly enables fast responses of a host to query messages, the router can also get the existing status of the multicast group members.

Example: Setting the maximum IGMP query response time to 20 seconds.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query- max-response-time 20

19.6.2.2.5 ip igmp query-timeout

Command: ip igmp query-timeout <*time_val*>
no ip igmp query-timeout

Function: Set the timeout interval for an interface to response to an IGMP query; the "**no ip igmp**

query-timeout" command restores the default setting.

Parameters: < ***time_val***> is the time to timeout an IGMP query, the valid range is 60 to 300 seconds..

Default: The default value is 265 seconds.

Command mode: Interface Mode

Usage Guide: In a shared network with several routers running IGMP, one switch will be selected as the querier for that shared network, the other switches act as timers monitoring the status of the querier; if no query packet from the querier is received after the query timeout time, a new switch will be elected to be the new querier.

Example: Configuring the interface timeout setting for IGMP queries to 100 seconds.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp query-timeout 100

19.6.2.2.6 ip igmp static-group

Command: ip igmp static-group <*A.B.C.D* >

no ip igmp static -group <*A.B.C.D* >

Function: Joins the interface to an IGMP static group; the "**no ip igmp static -group**" command cancels the join.

Parameters: **<*A.B.C.D*>** are the IP addresses for multicast groups.

Default: Not joined to static groups.

Command mode: Interface Mode

Usage Guide: After an interface joins a static group, then the interface will receive multicast packet about that static group regardless of whether there are actual receivers under the interface or not; for instance, if the local interface joins static group 224.1.1.1., then the local interface will keep receiving multicast packets about he group 224.1.1.1 regardless of whether there are receiver of not under the interface. Note the difference between this command and the "**ip igmp join-group**" command.

Example: Specifing interface vlan1 to join static group 224.1.1.1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp static-group 224.1.1.1

19.6.2.2.7 ip igmp version

Command: ip igmp version <*version*>

no ip igmp version

Function: Configures the IGMP version of the interface; the "**no ip igmp version**" command restores the default setting.

Parameters: **<*version*>** is the IGMP version configured, v1 and v2 are supported at present.

Default: The default version number is v2.

Command mode: Interface Mode

Usage Guide: This command is used to provide forward compatibility between different versions. It should be noted that v1 and v2 are not inter-connectable, and the same version of IGMP must be ensured for the same network.

Example: Configuring the IGMP running on the interface to version 1.

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip igmp version 1

19.6.3 Typical IGMP Scenario

As shown in the figure below, the Ethernet interfaces of SwitchA and SwitchB are added to the appropriate vlan, and PIM-DM protocol is enabled on each vlan interface.

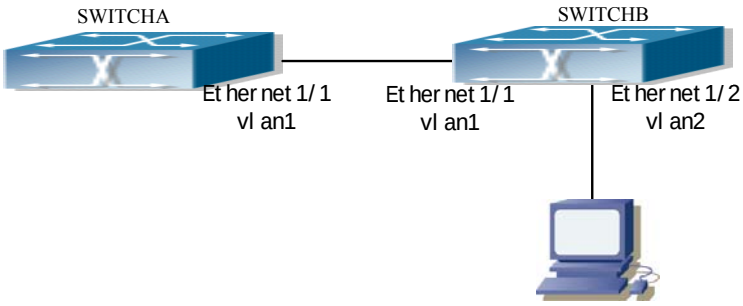


Fig 19-4 IGMP network topology

The followings are the configurations of SwitchA and SwitchB.

(1) Configuration of SWITCHA:

Switch (Config)#interface vlan 1

Switch(Config-If-Vlan1)#ip pim dense-mode

(2) Configuration of SWITCHB:

Switch(Config)#interface vlan1

Switch(Config-If-Vlan1)#ip pim dense-mode

Switch(Config-If-Vlan1)#exit

Switch(Config)#interface vlan2

Switch(Config-If-Vlan2)#ip pim dense-mode

Switch(Config-If-Vlan2)#ip igmp version 1

Switch(Config-If-Vlan2)#ip igmp query-timeout 150

19.6.4 IGMP Troubleshooting Help

1. Monitor and debug commands

2. IGMP Troubleshooting Help

19.6.4.1 Monitor and Debug Commands

19.6.4.1.1 show ip igmp groups

Command: show ip igmp groups [{<*ifname* | *group_addr*>}]

Function: Display sIGMP group information.

Parameters: <***ifname***> is the interface name, i.e., displays group information of the specified interface; <***group_addr***> is the group address, i.e., shows group information.

Default: Nothing is displayed by default

Command mode: Admin Mode

Example:

Switch#show ip igmp groups

IGMP Connect Group Membership (1 group(s) joined)

Group Address	Interface	Uptime	Expires	Last Reporter
239.255.255.250	Vlan123	02:57:30	00:03:36	123.1.1.2

Switch#

Displayed information	Explanation
Group Address	Multicast group IP address
Interface	Interface of the multicast group
Uptime	The up time of the multicast group
Expires	Rest time before the multicast group timeouts
Last Reporter	The host's last reported the multicast group

19.6.4.1.2 show ip igmp interface

Command: show ip igmp interface [<*ifname*>]

Function: Displays IGMP related information on the interface

Parameters: <***ifname***> is the interface name, i.e., displays IGMP information of the specified interface.

Default: Not displayed.

Command mode: Admin Mode

Example: Displaying IGMP information of Ethernet interface vlan1.

Switch # show ip igmp interface vlan1

Vlan1 is up, line protocol is up

Internet address is 192.168.1.11, subnet mask is 255.255.255.0

IGMP is enabled, I am querier

IGMP current version is V2

IGMP query interval is 125s

IGMP querier timeout is 265s

IGMP max query response time is 10s

Inboud IGMP access group is not set

Multicast routing is enable on interface

Multicast TTL threshold is 1

Multicast designed router (DR) is 192.168.1.22

Muticast groups joined by this system: 0

19.6.4.1.3 debug ip igmp event

Command: debug ip igmp event

Function: Enables the debug function for displaying IGMP events: the "**no**" format of this command disables this debug function.

Parameters: N/A.

Default: Disabled

Command mode: Admin Mode

Usage Guide: If detailed information about IGMP events is required, this debugging command can be used.

Example:

Switch# debug ip igmp event

igmp event debug is on

Switch# 01:04:30:56: IGMP: Group 224.1.1.1 on interface vlan1 timed out

19.6.4.1.4 debug ip igmp packet

Command: debug ip igmp packet

Function: Enables the IGMP packet debug function; the "**no debug ip ospf packet**" command disables this debug function.

Parameters: N/A.

Default: Disabled.

Command mode: Admin Mode

Usage Guide: If information about IGMP packets is required, this debugging command can be used.

Example:

Switch# debug ip igmp packet

igmp packet debug is on

Switch #02:17:38:58: IGMP: Send membership query on dvmrp2 for 0.0.0.0

02:17:38:58: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0

02:17:39:26: IGMP: Send membership query on vlan1 for 0.0.0.0

02:17:39:26: IGMP: Received membership query on dvmrp2 from 192.168.1.11 for 0.0.0.0

19.6.4.2 IGMP Troubleshooting

In configuring and using IGMP protocol, the IGMP protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use "show interface" command).
- ✧ Ensure at least one multicast protocol is enabled on the interface.
- ✧ Multicast protocols use unicast routes to perform RPF check, for this reason, the unicast route correctness must be ensured.

If IGMP problems persist after the abovementioned procedures, please run debug commands like

"debug ip igmp event/packet", and copy the debug information in 3 minute and send the information to Edge-Core technical service center.

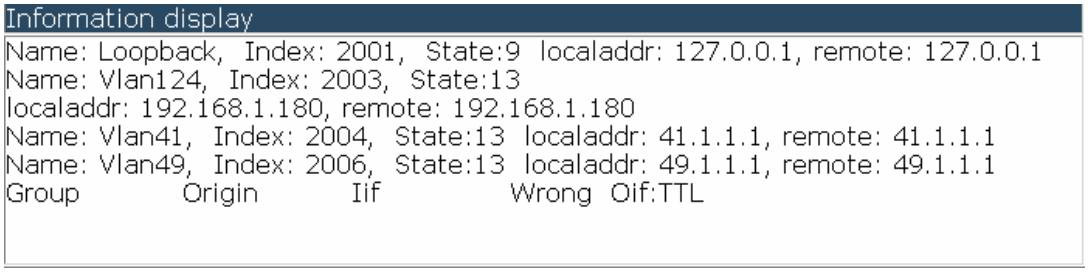
19.7 WEB MANAGEMENT

Click "root page" left content column "Multicast protocol configuration" to enter into multicast protocol configuration root node and make configuration for multicast protocol.

- Click Multicast common configuration to enter into multicast protocol public monitor mode
- Click PIM-DM configuration to enter into PIM-DM protocol configuration mode
- Click PIM-SM configuration to enter into PIM-SM protocol configuration mode
- Click DVMRP configuration to enter into DVMRP protocol configuration mode
- Click IGMP configuration to enter into IGMP protocol configuration mode
- Click Inspect and debug to enter into multicast protocol debug monitor mode

19.7.1 Multicast public monitor command

Example: In multicast protocol public monitor mode, click Show ip mroute to display IP multicast message forward item. This is the same as CLI command 19.2.1.1.1. No additional parameter configuration necessary. For the detailed information, please refer to 19.2.1.1.1：

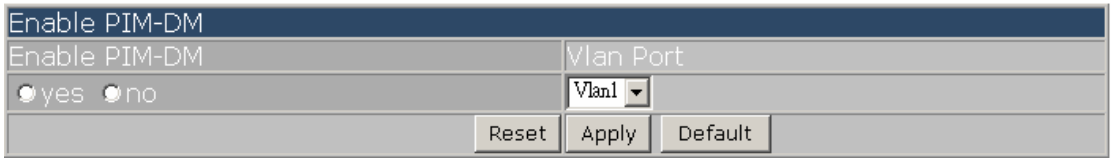

Information display
Name: Loopback, Index: 2001, State:9 localaddr: 127.0.0.1, remote: 127.0.0.1
Name: Vlan124, Index: 2003, State:13
localaddr: 192.168.1.180, remote: 192.168.1.180
Name: Vlan41, Index: 2004, State:13 localaddr: 41.1.1.1, remote: 41.1.1.1
Name: Vlan49, Index: 2006, State:13 localaddr: 49.1.1.1, remote: 49.1.1.1
Group Origin Iif Wrong Oif:TTL

19.7.2 PIM-DM configuration

19.7.2.1 Enable PIM-DM

In PIM-DM protocol configuration mode, click "Enable PIM-DM" to enable or disable PIM-DM protocol in layer 3 interface. This is the same as CLI command 19.3.2.3.

- Enable PIM-DM: yes means enable PIM-DM protocol；no means disable PIM-DM protocol
- Vlan Port: assigns layer 3 interface (select from scroll bar menu）
- Apply: runs according to configured parameter
- Default: disables assign layer 3 interface PIM-DM protocol

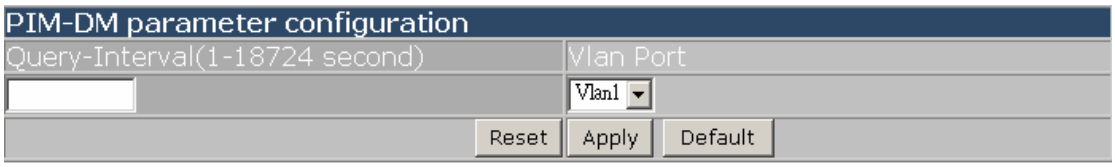


19.7.2.2 PIM-DM parameter configuration

Click "PIM-DM parameter configuration" to configure the PIM-DM running parameters for a specific layer 3 interface. This is the same as CLI command 19.3.2.4.

- Query-Interval — Configures local interface PIM-DM hello message interval time

- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — restores local interface PIM-DM hello message interval time to default

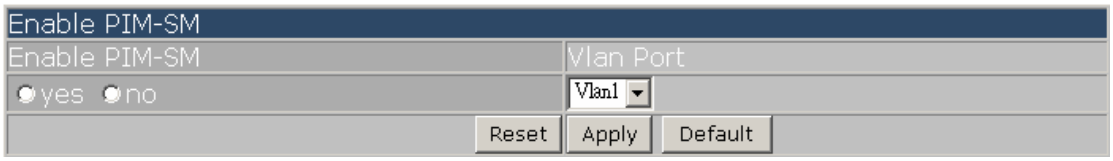


19.7.3 PIM-SM configuration

19.7.3.1 Enable PIM-SM

In PIM-SM protocol configuration mode, click "Enable PIM-SM" to enable or disable PIM-SM protocol in the layer 3 interface. This is the same as CLI command 19.4.2.2.1

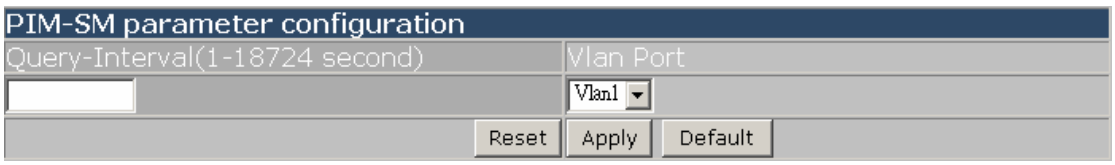
- Enable PIM-SM — yes means enable PIM-SM protocol; no means disable PIM-SM protocol
- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — disables assign layer 3 interface PIM-SM protocol



19.7.3.2 PIM-SM parameter configuration

Click "PIM-SM parameter configuration" to configure PIM-SM running parameter for a specific layer 3 interface. This is the same as CLI command 19.4.2.2.3

- Query-Interval — Configures local interface PIM-SM hello message interval time
- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — restores local interface PIM-DM hello message interval time to default



19.7.3.3 Set interface as PIM-SM BSR border

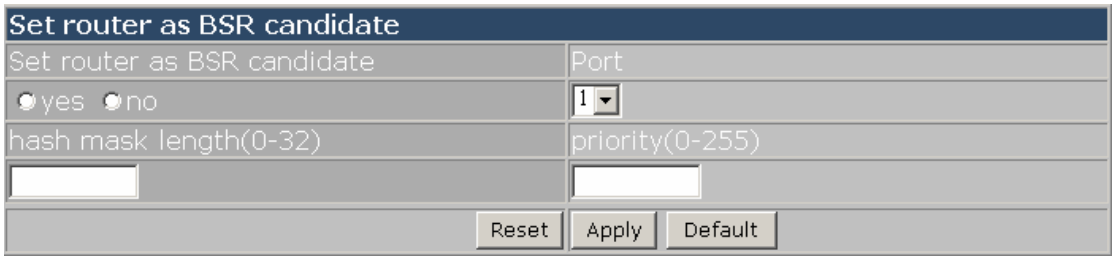
Click "Set interface as PIM-SM BSR border" to configure the PIM-SM domain border. In order to prevent BSR message diffusing this PIM-SM domain, configure the specific interface as PIM-SM domain border. This is the same as CLI command 19.4.2.2.2

- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — cancels local interface working as PIM-SM domain border

19.7.3.4 Set router as BSR candidate

Click Set router as BSR candidate for configure PIM-SM candidate BSR information ，for compete with other candidate BSR for BSR router. This is the same as CLI command 19.4.2.2.4

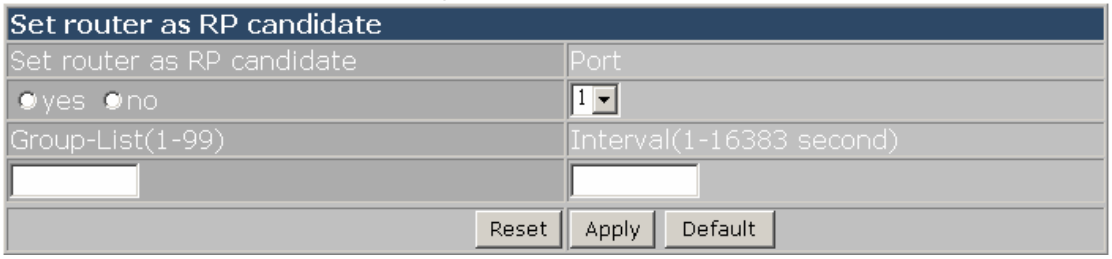
- Set router as BSR candidate — yes means configure the switch as PIM-SM domain candidate BSR; no means cancel switch to configure as candidate BSR
- Port — assign layer 3 interface VLAN ID（select from scroll bar menu）
- Hash mask length — assigns hash mask length
- Priority — assigns priority
- Apply — runs according to configured parameter
- Default — cancels switch to configure as candidate BSR



19.7.3.5 Set router as RP candidate

Click "Set router as RP candidate" to configure PIM-SM candidate RP information, to compete with other candidate RPs for RP router. This is the same as CLI command 19.4.2.2.5

- Set router as RP candidate — yes means configure switch as candidate PIM-SM RP; no means cancel RP configuration
- Port — assign layer 3 interface VLAN ID（select from scroll bar menu）
- Group-List — assign access-list ID
- Interval — assign sending candidate RP message interval
- Apply — run according to configured parameter
- Default — cancel RP configuration

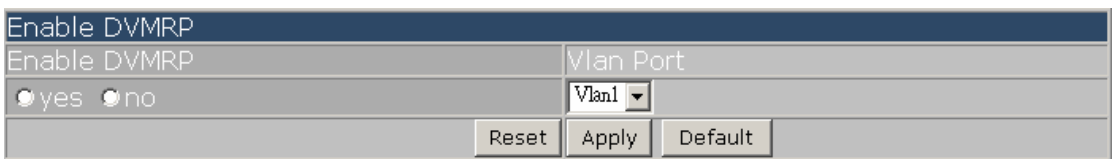


19.7.4 DVMRP configuration

19.7.4.1 Enable DVMRP

In DVMRP protocol configuration mode, click "Enable DVMRP" to enable or disable DVMRP protocol in specific interface. This is the sameas CLI command 19.5.2.2.2

- Enable DVMRP — yes means enable DVMRP protocol; no means disable DVMRP protocol
- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — disables DVMRP protocol

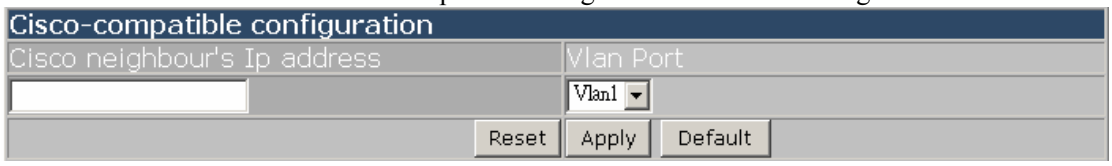


19.7.4.2 Cisco-compatible configuration

Click "Cisco-compatible configuration" to startup the connection with CISCO neighbor. This is the

sameas CLI command 19.5.2.2.1

- Cisco neighbor's IP address — assigns Cisco neighbor IP address
- Vlan Port — assigns layer 3 interface （select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — cancels the compatible configuration to the Cisco neighbor

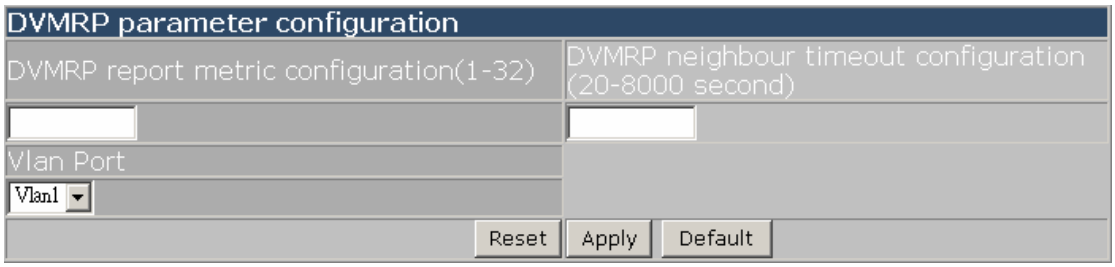


19.7.4.3 DVMRP parameter configuration

Click "DVMRP parameter configuration" to the configure DVMRP protocol interface configuration parameter. This is the sameas CLI command 19.5.2.2. and 19.5.2.2.5

- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- DVMRP report metric configuration — Configures interface DVMRP report message metric. This is the same as CLI command 19.5.2.2.4
- DVMRP neighbor timeout configuration — Configures interface DVMRP neighbor timeout. This is the same as CLI command 19.5.2.2.5
- Apply — runs according to configured parameter
- Default — restores the interface parameter to default (includes report message metric, neighbor timeout time）

Note：Because the page correspondence 2 PCS CLI command, a parameter error message will appear when. Only configure one or many parameters, it's not affected.

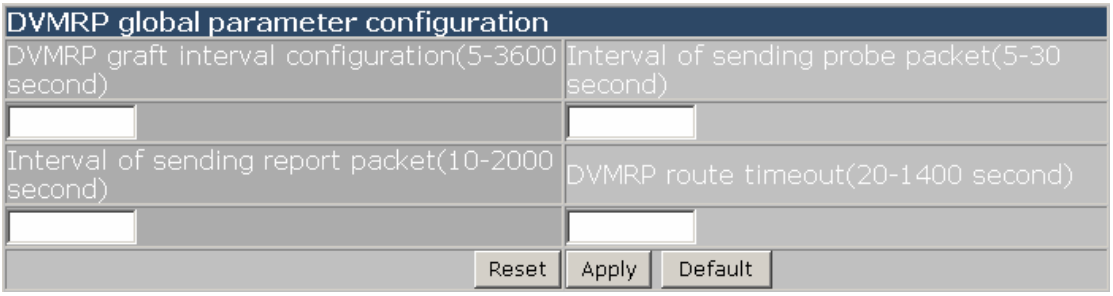


19.7.4.4 DVMRP global parameter configuration

Click "DVMRP global parameter configuration" to configure DVMRP protocol global configuration parameters. This is the same as 4 PCS CLI command 19.5.2.2.3, 19.5.2.2.6, 19.5.2.2.7, and 19.5.2.2.8

- DVMRP graft interval configuration — Configures DVMRP graft interval. This is the same as CLI command 19.5.2.2.3
- Interval of sending probe packet — Configures the interval of sending probe packet. This is the same as CLI command 19.5.2.2.6
- Interval of sending report packet — Configures the interval of sending report packet. This is the same as CLI command 19.5.2.2.7
- DVMRP route timeout —configures DVMRP route timeout. This is the same as CLI command 19.5.2.2.8
- Apply — runs according to configured parameter
- Default — restores the global configuration parameter to default (includes sending graft, probe, report message interval, dvmrp route timeout）

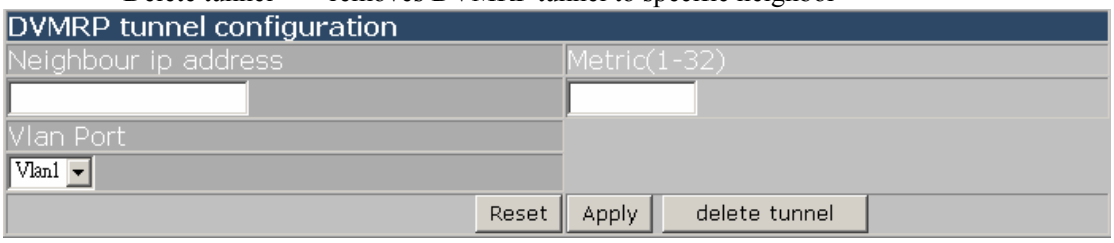
Note：Because the page correspondence 4 PCS CLI command，it will appear error parameter message when only configure one or many parameter, it's not affected.



19.7.4.5 DVMRP tunnel configuration

Click "DVMRP tunnel configuration to create", repeal the tunnel which to neighbor DVMRP tunnel . This is the same as CLI command 19.5.2.2.9

- Neighbor ip address — remote neighbor IP address
- Metric — tunnel interface metric
- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — creates DVMRP tunnel to specific neighbor
- Delete tunnel — removes DVMRP tunnel to specific neighbor



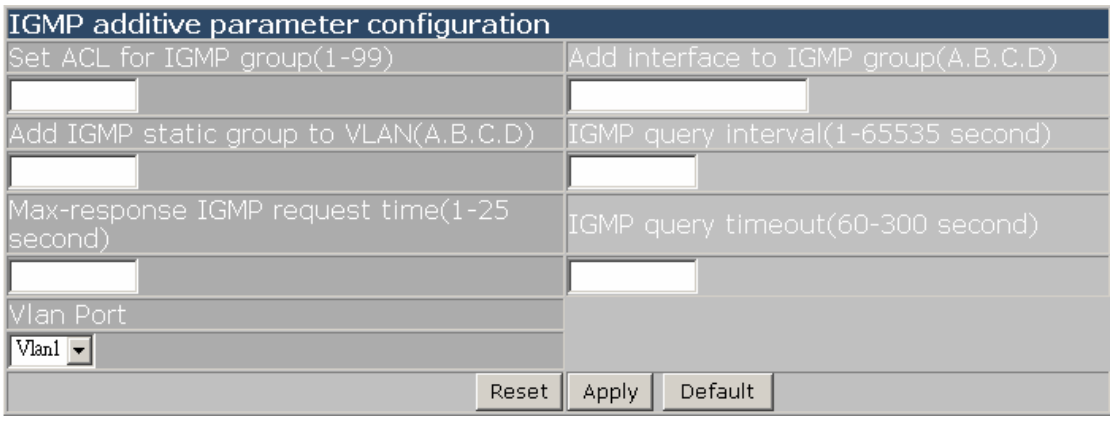
19.7.5 IGMP configuration

19.7.5.1 IGMP additive parameter configuration

In "IGMP protocol configuration mode", click "IGMP additive parameter configuration" to configure IGMP protocol interface parameters. This is the same as 6 PCS CLI command 19.6.2.2.1, 19.6.2.2.2, 19.6.2.2.3, 19.6.2.2.4, 19.6.2.2.5, 19.6.2.2.6

- Set Acl for IGMP group — Configures interface filter qualifications to IGMP group. This is the same as CLI command 19.6.2.2.1
- Add interface to IGMP group — Configures interface to join some IGMP group. This is the same as CLI command 19.6.2.2.2
- Add IGMP static group to VLAN — Configures interface join some IGMP static group. This is the same as CLI command 19.6.2.2.6
- IGMP query interval — Configures IGMP query interval. This is the same as CLI command 19.6.2.2.3
- Max-response IGMP request time — Configures max-response IGMP request time. This is the same as CLI command 19.6.2.2.4
- IGMP query timeout — Configures IGMP query timeout. This is the same as CLI command 19.6.2.2.5
- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — restores the interface configuration parameter to default (including group filter qualification, query interval, maximum response time, query timeout)，if input relevant group address for static group domain and join group domain，it will cancel static group or（and）join group in interface.

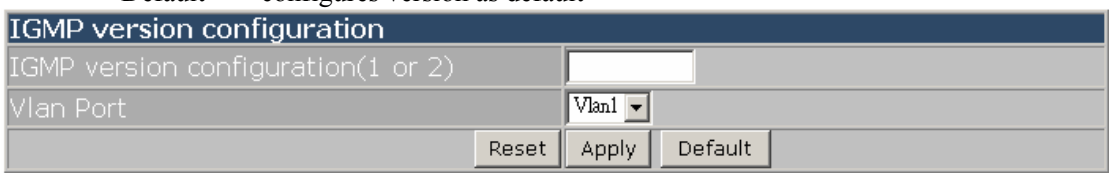
Note：Because the page correspondence 6 PCS CLI command，A error parameter message will appear when only configure one or many parameter，it's not affected.



19.7.5.2 IGMP version configuration

Click "IGMP version configuration" to configure interface IGMP protocol version. This is the same as CLI command 19.6.2.2.7

- IGMP version configuration — assigns version
- Vlan Port — assigns layer 3 interface（select from scroll bar menu）
- Apply — runs according to configured parameter
- Default — configures version as default



19.7.6 Multicast monitor configuration

19.7.6.1 Show ip pim interface

In multicast protocol monitor mode, click "Show ip pim interface" to display the PIM interface information. This is the same as CLI command 19.4.4.1.2

19.7.6.2 Show ip pim mroute dm

Click "Show ip pim mroute dm" to display the PIM-DM message forwarding item. This is the same as CLI command 19.3.4.2

19.7.6.3 Show ip pim neighbor

Click "Show ip pim neighbor" to display PIM interface neighbor information. This is the same as CLI command 19.3.4.3

19.7.6.4 Show ip pim bsr-router

Click "Show ip pim bsr-router" to display the running PIM-SM protocol BSR information. This is the same as CLI command 19.4.4.1.1

19.7.6.5 Show ip pim mroute sm

Click "Show ip pim mroute sm" to display PIM-SM message forwarding item. This is the same as CLI command 19.4.4.1.3

19.7.6.6 Show ip pim rp

Click "Show ip pim rp to display RP" interrelated information of PIM. This is the same as CLI command 19.4.4.1.5

19.7.6.7 Show ip dvmrp mroute

Click “Show ip dvmrp mroute” to display DVMRP message forward item. This is the same as CLI command 19.5.4.1.1

19.7.6.8 Show ip dvmrp neighbor

Click “Show ip dvmrp neighbor” to display DVMRP neighbor information. This is the same as CLI command 19.5.4.1.2

19.7.6.9 Show ip dvmrp route

Click “Show ip dvmrp route” to display DVMRP route information. This is the same as CLI command 19.5.4.1.3

19.7.6.10 Show ip dvmrp tunnel

Click “Show ip dvmrp tunnel” to display DVMRP tunnel information. This is the same as CLI command 19.5.4.1.4

Chapter20 802.1x Configuration

20.1 Introduction to 802.1x

IEEE 802.1x is a port-based network access management method, which authenticates and manages the accessing devices on the physical access level of the LAN device. The physical access level here are the ports of the switch. If the users' devices connected to such ports can be authenticated, access to resources in the LAN is allowed; otherwise, access will be denied, which is essentially the same as disconnecting physically.

IEEE 802.1x defines a port-based network access management protocol. It should be noted that the protocol applies to point-to-point connection between the accessing device and the access port, where the port can be either a logical port or a physical port. Typically, one physical port of the switch connects with one terminal device (physical port-based) only.

The architecture of IEEE 802.1x is shown below:

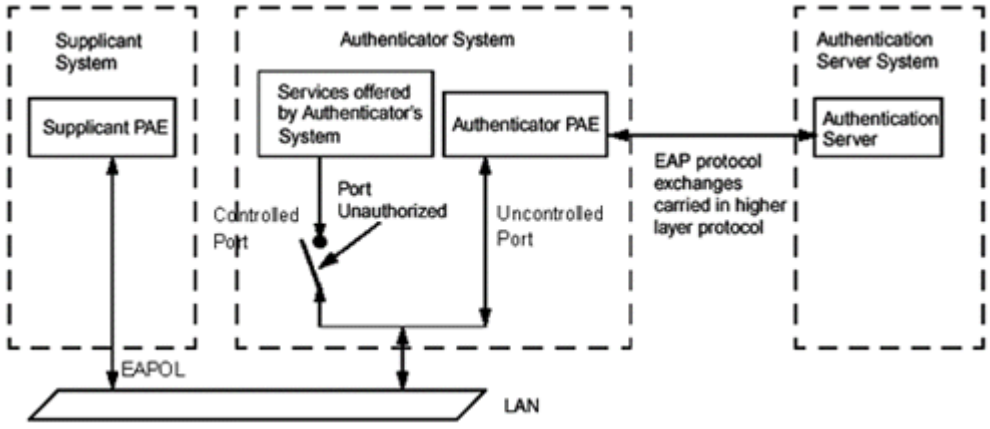


Fig 20-1 802.1x architecture

As shown in the above figure, the IEEE 802.1x architecture consists of three parts:

- Supplicant System (user access devices)
- Authenticator System (access management unit)
- Authentication Server System (the authenticating server)

EAPOL protocol defined by IEEE 802.1x runs between the user access device (PC) and access management unit (access switch); and EAP protocol is also used between the access management unit and authenticating server. EAP packets encapsulates the authenticating data. The EAP packet is conveyed in the packets of the higher layer protocols such as RADIUS to pass through complex network to the authenticating server.

The ports provided by the port-based network access management device end are divided into two virtual port types: managed port and non-managed port. A non-managed port is always in the connected status for both in and out directions to transfer EAP authenticating packets. A managed port will be in the connected status when authorized to transfer commutation packets; and is shutdown when not authorized, and cannot transfer any packets.

In the IEEE 802.1x application environment, ES4704BD is used as the access management unit, and the user connection device is the device with 802.1x client software. An authenticating server usually reside in the Carrier's AAA center and usually is a Radius server.

The authentication function of port-based IEEE 802.1x is limited when multiple user access devices connect to one physical port, since the authentication will not be able to tell the difference between user access, MAC-based IEEE 802.1x authentication is implemented in ES4704BD for better security and management. Only authenticated user access devices connecting to the same physical port can access the network, the unauthorized devices will not be able to access the network. In this way, even if multiple terminals are connected via one physical port, ES4704BD can still authenticate and manage each user access device individually.

The maximum authenticating user number supported by ES4704BD is 4,000. It is recommended to keep the authenticating user number under 2,000.

20.2 802.1x Configuration

20.2.1 802.1x Configuration Task Sequence

1. Enable IEEE 802.1x function: of the switch.
2. Access management unit property configuration
   1) Configure port authentication status
   2) Configure access management method for the port: MAC-based or port-based.
   3) Configure expanded 802.1x function: for the switch.
3. User access devices related property configuration (optional)
4. RADIUS server related property configuration
   1) Configure RADIUS authentication key.
   2) Configure RADIUS Server
   3) Configure RADIUS Service parameters.

1. Enable 802.1x function: of the switch.

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	Enables the AAA authentication function in the switch; the "**no aaa enable**" command disables the AAA authentication function.
aaa-accounting enable **no aaa-accounting enable**	Enables the accounting function in the switch; the "**no aaa-accounting enable**" command disables the accounting function
dot1x enable **no dot1x enable**	Enables the 802.1x function in the switch and ports; the "**no dot1x enable**" command disables the 802.1x function.
dot1x privateclient enable **no dot1x privateclient enable**	Enables the switch to force client software to use Edge-Core's proprietary 802.1x authentication packet format; the "**no dot1x privateclient enable**" command disables the function and allow the client software to use standard 802.1x authentication packet format.

2. Access management unit property configuration

1) Configure port authentication status

Command	Explanation
Port Mode	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Sets the 802.1x authentication mode; the "**no dot1x port-control**" command restores the default setting.

2) Configure port access management method

Command	Explanation
Port Mode	
dot1x port-method {macbased | portbased} **no dot1x port-method**	Sets the port access management method; the "**no dot1x port-method**" command restores MAC-based access management.
dot1x max-user <*number*> **no dot1x max-user**	Sets the maximum number of access users for the specified port; the "**no dot1x max-user**" command restores the default setting of allowing 1 user.

3) Configure expanded 802.1x function: for the switch.

Command	Explanation
Global Mode	
dot1x macfilter enable **no dot1x macfilter enable**	Enables the 802.1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the 802.1x address filter function.
dot1x accept-mac <*mac-address*> [interface <*interface-name*>] **no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**	Adds 802.1x address filter table entry, the "**no dot1x accept-mac**" command deletes 802.1x filter address table entries.
dot1x eapor enable **no dot1x eapor enable**	Enables the EAP relay authentication function in the switch; the "**no dot1x eapor enable**" command sets EAP local end authentication.

3. Supplicant related property configuration

Command	Explanation
Global Mode	
dot1x max-req <*count*> **no dot1x max-req**	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response, the "**no dot1x max-req**" command restores the default setting.
dot1x re-authentication **no dot1x re-authentication**	Enables periodical supplicant authentication; the "**no dot1x re-authentication**" command disables this function.
dot1x timeout quiet-period <*seconds*> **no dot1x timeout quiet-period**	Sets time to keep silent on port authentication failure; the "**no dot1x timeout quiet-period**" command restores the default value.
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	Sets the supplicant re-authentication interval; the "**no dot1x timeout re-authperiod**" command restores the default setting.
dot1x timeout tx-period <*seconds*> **no dot1x timeout tx-period**	Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.
Admin Mode	
dot1x re-authenticate [interface <*interface-name*>]	Enables IEEE 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

4. Authentication Server (RADIUS server) related property configuration

1) Configure RADIUS authentication key.

Command	Explanation

Global Mode	
radius-server key <*string*> no radius-server key	Specifies the key for RADIUS server; the **"no radius-server key"** command deletes the key for RADIUS server.

2) Configuring RADIUS Server

Command	Explanation
Global Mode	
radius-server authentication host <*IPaddress*> [[port {<*portNum*>}] [primary]] **no radius-server authentication host <*IPaddress*>**	Specifies the IP address and listening port number for RADIUS authentication server; the "**no radius-server authentication host <*IPaddress*>**" command deletes the RADIUS server
radius-server accounting host <IPaddress> [[port {<*portNum*>}] [primary]] **no radius-server accounting host <*IPaddress*>**	Specifies the IP address and listening port number for RADIUS accounting server; the "**no radius-server authentication host <*IPaddress*>**" command deletes the RADIUS server

3) Configure RADIUS Service parameters.

Command	Explanation
Global Mode	
radius-server dead-time <*minutes*> **no radius-server dead-time**	Configures the restore time when RADIUS server is down; the "**no radius-server dead-time**" command restores the default setting.
radius-server retransmit <*retries*> **no radius-server retransmit**	Configures the re-transmission times for RADIUS; the "**no radius-server retransmit**" command restores the default setting
radius-server timeout <*seconds*> **no radius-server timeout**	Configures the timeout timer for RADIUS server; the "**no radius-server timeout**" command restores the default setting.

20.2.2 802.1x Configuration Commands

20.2.2.1 aaa enable

Command: aaa enable

no aaa enable

Function: Enables the AAA authentication function in the switch; the "**no AAA enable**" command disables the AAA authentication function.

Command mode: Global Mode

Parameters: N/A.

Default: AAA authentication is not enabled by default.

Usage Guide: The AAA authentication for the switch must be enabled first to enable IEEE 802.1x authentication for the switch.

Example: Enabling AAA function for the switch.

Switch(Config)#aaa enable

20.2.2.2 aaa-accounting enable

Command: aaa-accounting enable

no aaa-accounting enable

Function: Enables the AAA accounting function in the switch: the "**no aaa-accounting enable**" command disables the AAA accounting function.

Command mode: Global Mode

Default: AAA accounting is not enabled by default.

Usage Guide: When accounting is enabled in the switch, accounting will be performed according to the traffic or online time for port the authenticated user is using. The switch will send an "accounting started" message to the RADIUS accounting server on starting the accounting, and an accounting packet for the online user to the RADIUS accounting server every five seconds, and an "accounting stopped" message is sent to the RADIUS accounting server on accounting end. Note: The switch send the "user offline" message to the RADIUS accounting server only when accounting is enabled, the "user offline" message will not be sent to the RADIUS authentication server.

Example: Enabling AAA accounting for the switch.

Switch(Config)#aaa-accounting enable

20.2.2.3 dot1x accept-mac

Command: dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

Function: Adds a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The "**no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**" command deletes the entry from dot1x address filter table.

Parameters: **<*mac-address*>** stands for MAC address; **<*interface-name*>** for interface name and port number.

Command mode: Global Mode

Default: N/A.

Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.

Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/5.

Switch(Config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/5

20.2.2.4 dot1x eapor enable

Command: dot1x eapor enable

no dot1x eapor enable

Function: Enables the EAP relay authentication function in the switch; the "**no dot1x eapor enable**" command sets EAP local end authentication.

Command mode: Global Mode

Default: EAP relay authentication is used by default.

Usage Guide: The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.

Example: Setting EAP local end authentication for the switch.

Switch(Config)#no dot1x eapor enable

20.2.2.5 dot1x enable

Command: dot1x enable

no dot1x enable

Function: Enables the 802.1x function in the switch and ports: the "**no dot1x enable**" command disables the 802.1x function.

Command mode: Global Mode and Interface Mode.

Default: 802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.

Usage Guide: The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.

Example: Enabling the 802.1x function of the switch and enable 802.1x for port 1/12.

Switch(Config)#dot1x enable

Switch(Config)#interface ethernet 1/12

Switch(Config-Ethernet0/0/12)#dot1x enable

20.2.2.6 dot1x privateclient enable

Command: dot1x privateclient enable

no dot1x privateclient enable

Function: Enables the switch to force client software to use Edge-Core's proprietary 802.1x authentication packet format; the "**no dot1x privateclient enable**" command disables the function and allow the client software to use standard 802.1x authentication packet format.

Command mode: Global Mode

Default: Proprietary authentication is not supported by the switch.

Usage Guide: To implement the Edge-Core overall solution, Edge-Core proprietary 802.1x

authentication packets support must be enabled in the switch, otherwise many application would not be available. For detailed information, please refer to the introduction of Edge-Core Overall Solution, Standard 802.1x client would not be authenticated if Edge-Core proprietary 802.1x authentication packet format is enforced for client software by the switch.

Example: Enabling the switch to force client software to use Edge-Core proprietary 802.1x authentication packet format.

Switch(Config)#dot1x privateclient enable

20.2.2.7 dot1x macfilter enable

Command: dot1x macfilter enable

no dot1x macfilter enable

Function: Enables the dot1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the dot1x address filter function.

Command mode: Global Mode

Default: dot1x address filter is disabled by default.

Usage Guide: When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.

Example: Enabling dot1x address filter function for the switch.

Switch(Config)#dot1x macfilter enable

20.2.2.8 dot1x max-req

Command: dot1x max-req <*count*>

no dot1x max-req

Function: Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response; the "**no dot1x max-req**" command restores the default setting.

Parameters: < *count*> is the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10.

Command mode: Global Mode

Default: The default maximum for retransmission is 2.

Usage Guide: The default value is recommended in setting the EAP request/ MD5 retransmission times.

Example: Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.

Switch(Config)#dot1x max-req 5

20.2.2.9 dot1x max-user

Command: dot1x max-user <*number*>

no dot1x max-user

Function: Sets the maximum users allowed to connect to the port; the "**no dot1x max-user**" command restores the default setting.

Parameters: < *number*> is the maximum users allowed, the valid range is 1 to 254.

Command mode: Port configuration Mode.

Default: The default maximum user allowed is 1.

Usage Guide: This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.

Example: Setting port 1/3 to allow 5 users.

Switch(Config-Ethernet1/3)#dot1x max-user 5

20.2.2.10 dot1x port-control

Command: dot1x port-control {auto|force-authorized|force-unauthorized }

no dot1x port-control

Function: Sets the 802.1x authentication status; the "**no dot1x port-control**" command restores the default setting.

Parameters: auto enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant; **force-authorized** sets port to authorized status, unauthenticated data is allowed to pass through the port; **force-unauthorized** will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port.

Command mode: Port configuration Mode

Default: When 802.1x is enabled for the port, **force authorized** is set by default.

Usage Guide: If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to **auto**.

Example: Setting port1/1 to require 802.1x authentication mode.

Switch(Config)#interface ethernet 1/1

Switch(Config-Ethernet1/1)#dot1x port-control auto

20.2.2.11 dot1x port-method

Command: dot1x port-method {macbased | portbased}

no dot1x port-method

Function: Sets the access management method for the specified port; the "**no dot1x port-method**" command restores the default access management method.

Parameters: macbased sets the MAC-based access management method; **portbased** sets port-based access management.

Command mode: Port configuration Mode

Default: MAC-based access management is used by default.

Usage Guide: MAC-based access management is better than port-based access management in both security and management, port-based access management is suggested only for special usages.

Example: Setting port-based access management for port 1/4.

Switch(Config-Ethernet1/4)#dot1x port-method portbased

20.2.2.12 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>]

Function: Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a

specified port.

Parameters: <***interface-nam***> stands for port number, omitting the parameter for all ports.

Command mode: Admin Mode

Usage Guide: This command is an Admin Mode command. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.

Example: Enabling real-time re-authentication on port 1/8.

Switch#dot1x re-authenticate interface ethernet 1/8

20.2.2.13 dot1x re-authentication

Command: dot1x re-authentication

no dot1x re-authentication

Function: Enables periodical supplicant authentication; the "**no dot1x re-authentication**" command disables this function.

Command mode: Global Mode

Default: Periodical re-authentication is disabled by default.

Usage Guide: When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.

Example: Enabling the periodical re-authentication for authenticated users.

Switch(Config)#dot1x re-authentication

20.2.2.14 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>

no dot1x timeout quiet-period

Function: Sets time to keep silent on supplicant authentication failure; the "**no dot1x timeout quiet-period**" command restores the default value.

Parameters: <***seconds***> is the silent time for the port in seconds, the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 10 seconds.

Usage Guide: Default value is recommended.

Example: Setting the silent time to 120 seconds.

Switch(Config)#dot1x timeout quiet-period 120

20.2.2.15 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <*seconds*>

no dot1x timeout re-authperiod

Function: Sets the supplicant re-authentication interval; the "**no dot1x timeout re-authperiod**" command restores the default setting.

Parameters: <***seconds***> is the interval for re-authentication, in seconds, the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 3600 seconds.

Usage Guide: dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.

Example: Setting the re-authentication time to 1200 seconds.

Switch(Config)#dot1x timeout re-authperiod 1200

20.2.2.16 dot1x timeout tx-period

Command: dot1x timeout tx-period <*seconds*>

no dot1x timeout tx-period

Function: Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.

Parameters: <***seconds***> is the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 30 seconds.

Usage Guide: Default value is recommended.

Example: Setting the EAP request frame re-transmission interval to 1200 seconds.

Switch(Config)#dot1x timeout tx-period 1200

20.2.2.17 radius-server accounting host

Command: radius-server accounting host <*ip-address*> [port <*port-number*>] [primary]

no radius-server accounting host <*ip-address*>

Function: Specifies the IP address and listening port number for RADIUS accounting server; the "**no radius-server authentication host <*IPaddress*>**" command deletes the RADIUS accounting server

Parameters: <***ip-address***> stands for the server IP address; <***port-number***> for server listening port number from 0 to 65535; **primary** for primary server. Multiple RADIUS sever can be configured and would be available. RADIUS server will be searched by the configured order if **primary** is not configured, otherwise, the specified RADIUS server will be used first.

Command mode: Global Mode

Default: No RADIUS accounting server is configured by default.

Usage Guide: This command is used to specify the IP address and port number of the specified RADIUS server for switch accounting, multiple command instances can be configured. The <***port-number***> parameter is used to specify accounting port number, which must be the same as the specified accounting port in the RADIUS server; the default port number is 1813. If this port number is set to 0, accounting port number will be generated at random and can result in invalid configuration. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the switch will send accounting packets to all the configured accounting

servers, and all the accounting servers can be backup servers for each other. If **primary** is specified, then the specified RADIUS server will be the primary server.

Example: Sets the RADIUS accounting server of IP address to 100.100.100.60 as the primary server, with the accounting port number as 3000.

Switch(Config)#radius-server accounting host 100.100.100.60 port 3000 primary

20.2.2.18 radius-server authentication host

Command: radius-server authentication host <*ip-address*> [port <*port-number*>] [primary]
no radius-server authentication host <*ip-address*>

Function: Specifies the IP address and listening port number for the RADIUS server; the "**no radius-server authentication host <*IPaddress*>**" command deletes the RADIUS authentication server

Parameters: **<*ip-address*>** stands for the server IP address; **<*port-number*>** for listening port number, from 0 to 65535, where 0 stands for non-authentication server usage; **primary** for primary server.

Command mode: Global Mode

Default: No RADIUS authentication server is configured by default.

Usage Guide: This command is used to specify the IP address and port number of the specified RADIUS server for switch authentication, multiple command instances can be configured. The port parameter is used to specify authentication port number, which must be the same as the specified authentication port in the RADIUS server, the default port number is 1812. If this port number is set to 0, the specified server is regard as non-authenticating. This command can be used repeatedly to configure multiple RADIUS servers communicating with the switch, the configured order is used as the priority for the switch authentication server. If **primary** is specified, then the specified RADIUS server will be the primary server.

Example: Setting the RADIUS authentication server address as 200.1.1.1.

Switch(Config)#radius-server authentication host 200.1.1.1

20.2.2.19 radius-server dead-time

Command: radius-server dead-time <*minutes*>
no radius-server dead-time

Function: Configures the restore time when RADIUS server is down; the "**no radius-server dead-time**" command restores the default setting.

Parameters: **< *minute* >** is the down -restore time for RADIUS server in minutes, the valid range is 1 to 255.

Command mode: Global Mode

Default: The default value is 5 minutes.

Usage Guide: This command specifies the time to wait for the RADIUS server to recover from inaccessible to accessible. When the switch acknowledges a server to be inaccessible, it marks that server as having invalid status, after the interval specified by this command; the system resets the status for that server to valid.

Example: Setting the down-restore time for RADIUS server to 3 minutes.

Switch(Config)#radius-server dead-time 3

20.2.2.20 radius-server key

Command: radius-server key <*string*>

no radius-server key

Function: Specifies the key for the RADIUS server (authentication and accounting); the "no radius-server key" command deletes the key for RADIUS server.

Parameters: <*string*> is a key string for RADIUS server, up to 16 characters are allowed.

Command mode: Global Mode

Usage Guide: The key is used in the encrypted communication between the switch and the specified RADIUS server. The key set must be the same as the RADIUS server set, otherwise, proper RADIUS authentication and accounting will not perform properly.

Example: Setting the RADIUS authentication key to be "test".

Switch(Config)# radius-server key test

20.2.2.21 radius-server retransmit

Command: radius-server retransmit <*retries*>

no radius-server retransmit

Function: Configures the re-transmission times for RADIUS authentication packets; the "**no radius-server retransmit**" command restores the default setting

Parameters: <*retries*> is a retransmission times for RADIUS server, the valid range is 0 to 100.

Command mode: Global Mode

Default: The default value is 3 times.

Usage Guide: This command specifies the retransmission time for a packet without a RADIUS server response after the switch sends the packet to the RADIUS server. If authentication information is missing from the authentication server, AAA authentication request will need to be re-transmitted to the authentication server. If AAA request retransmission count reaches the retransmission time threshold without the server responding, the server will be considered to as not working, the switch sets the server as invalid.

Example: Setting the RADIUS authentication packet retransmission time to five times.

Switch(Config)# radius-server retransmit 5

20.2.2.22 radius-server timeout

Command: radius-server timeout <*seconds*>

no radius-server timeout

Function: Configures the timeout timer for RADIUS server; the "**no radius-server timeout**" command restores the default setting.

Parameters: <*seconds*> is the timer value (second) for RADIUS server timeout, the valid range is 1 to 1000.

Command mode: Global Mode

Default: The default value is 3 seconds.

Usage Guide: This command specifies the interval for the switch to wait RADIUS server response. The switch waits for corresponding response packets after sending RADIUS Server request packets. If RADIUS server response is not received in the specified waiting

time, the switch resends the request packet or sets the server as invalid according to the current conditions.

Example: Setting the RADIUS authentication timeout timer value to 30 seconds.

Switch(Config)# radius-server timeout 30

20.3 802.1x Application Example

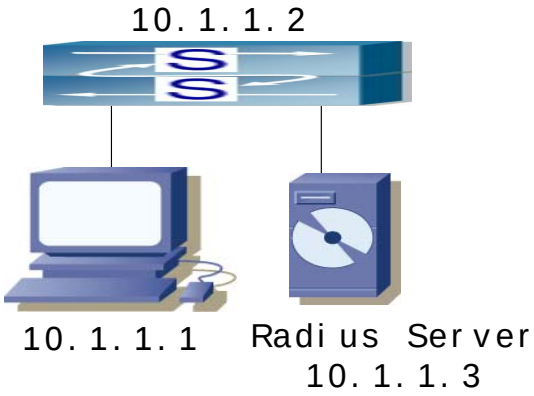


Fig 20-2 IEEE 802.1x Configuration Example Topology

The PC is connecting to port 1/2 of the switch; IEEE 802.1x authentication is enabled on port 1/2; the access mode is the default MAC-based authentication. The switch IP address is 10.1.1.2. Any port other than port 1/2 is used to connect to RADIUS authentication server, which has an IP address of 10.1.1.3, and use the default port 1812 for authentication and port 1813 for accounting. IEEE 802.1x authentication client software is installed on the PC and is used in IEEE 802.1x authentication.

The configuration procedures are listed below:

Switch(Config)#interface vlan 1

Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0

Switch(Config-if-vlan1)#exit

Switch(Config)#radius-server authentication host 10.1.1.3

Switch(Config)#radius-server accounting host 10.1.1.3

Switch(Config)#radius-server key test

Switch(Config)#aaa enable

Switch(Config)#aaa-accounting enable

Switch(Config)#dot1x enable

Switch(Config)#interface ethernet 1/2

Switch(Config-Ethernet1/2)#dot1x enable

Switch(Config-Ethernet1/2)#dot1x port-control auto

Switch(Config-Ethernet1/2)#exit

20.4 802.1x Troubleshooting

20.4.1 802.1x Debug and Monitor Commands

20.4.1.1 show aaa config

Command: show aaa config

Function: Displays the configured commands for the switch as a RADIUS client.

Command mode: Admin Mode

Usage Guide: Displays whether AAA authentication, accounting are enabled and information for key, authentication and accounting server specified.

Example:

Switch#show aaa config（For Boolean value, 1 stands for TRUE and 0 for FALSE）

---------- AAA config data ----------

Is Aaa Enabled = 1
Is Account Enabled= 1
MD5 Server Key = aa
authentication server sum = 2
authentication server[0].Host IP = 30.1.1.30
.Udp Port = 1812
.Is Primary = 1
.Is Server Dead = 0
.Socket No = 0
authentication server[1].Host IP = 192.168.1.218
.Udp Port = 1812
.Is Primary = 0
.Is Server Dead = 0
.Socket No = 0
accounting server sum = 2
accounting server[0].Host IP = 30.1.1.30
.Udp Port = 1813
.Is Primary = 1
.Is Server Dead = 0
.Socket No = 0
accounting server[1].Host IP = 192.168.1.218

.Udp Port = 1813

.Is Primary = 0

.Is Server Dead = 0

.Socket No = 0

Time Out = 3

Retransmit = 3

Dead Time = 5

Account Time Interval = 0

Displayed information	Description
Is AAA Enabled	Indicates whether AAA authentication is enabled or not. 1 for enable and 0 for disable.
Is Account Enabled	Indicates whether AAA accounting is enabled or not. 1 for enable and 0 for disable.
MD5 Server Key	Displays the key for RADIUS server.
authentication server sum	The number of authentication servers.
authentication server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	Displays the authentication server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.
accounting server sum	The number of accounting servers.
accounting server[X].Host IP .Udp Port .Is Primary .Is Server Dead .Socket No	Displays the accounting server number and corresponding IP address, UDP port number, Primary server or not, down or not, and socket number.
Time Out	Displays the timeout value for RADIUS server.
Retransmit	Displays the retransmission times for RADIUS server authentication packets.
Dead Time	Displays the down-restoration time for RADIUS server.
Account Time Interval	Displays accounting time interval.

20.4.1.2 show aaa authenticated-user

Command: show aaa authenticated-user

Function: Displays the authenticated users online.

Command mode: Admin Mode

Usage Guide: Usually the administrator is concerned only with the online user information, the other information displayed is used for troubleshooting by technical support.

Example:

```
Switch#show aaa authenticated-user
------------------------ authenticated users -----------------------------
  UserName    Retry RadID Port EapID ChapID OnTime        UserIP              MAC
-------------------------------------------------------------------------------

                ---------- total: 0 ----------
```

20.4.1.3 show aaa authenticating-user

Command: show aaa authenticating-user

Function: Display the authenticating users.

Command mode: Admin Mode

Usage Guide: Usually the administrator concerns only information about the authenticating user , the other information displays is used for troubleshooting by the technical support.

Example:

```
Switch#show aaa authenticating-user

------------------------- authenticating users -----------------------------
    User-name      Retry-time   Radius-ID      Port    Eap-ID Chap-ID Mem-Addr      State
-------------------------------------------------------------------------------

                ---------- total: 0 ----------
```

20.4.1.4 show radius count

Command: show radius {authencated-user|authencating-user} count

Function: Displays the statistics for users of RADIUS authentication.

Parameters: **authencated-user** displays the authenticated users online; **authencating-user** displays the authenticating users.

Command mode: Admin Mode

Usage Guide: The statistics for RADIUS authentication users can be displayed with the “show radius count” command.

Example:

1. Display the statistics for RADIUS authenticated users.

```
Switch #show radius authencated-user count
      ---------- Radius user statistic----------
The authencated online user num is:         1
```

The total user num is: 1

2. Display the statistics for RADIUS authenticated users and others.

Switch #sho radius authencating-user count

---------- Radius user statistic----------

The authencating user num is: 0

The stopping user num is: 0

The stopped user num is: 0

The total user num is: 1

20.4.1.5 show dot1x

Command: show dot1x [interface <*interface-list*>]

Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.

Parameters: **<*interface-list*>** is the port list. If no parameter is specified, information for all ports is displayed.

Command mode: Admin Mode

Usage Guide: The dot1x related parameter and dot1x information can be displayed with "show dot1x" command.

Example:

1. Display information about dot1x global parameter for the switch.

Switch#show dot1x

Global 802.1x Parameters

reauth-enabled	no
reauth-period	3600
quiet-period	10
tx-period	30
max-req	2
authenticator mode	passive

Mac Filter Disable

MacAccessList :

dot1x-EAPoR Enable

dot1x-privateclient Disable

802.1x is enabled on ethernet 1

Authentication Method:Port based

Status	Authorized
Port-control	Auto

Supplicant 00-03-0F-FE-2E-D3

Authenticator State Machine

State Authenticated

Backend State Machine

State Idle

Reauthentication State Machine

State Stop

Displayed information	Explanation
Global 802.1x Parameters	Global 802.1x parameter information
reauth-enabled	Whether re-authentication is enabled or not
reauth-period	Re-authentication interval
quiet-period	Silent interval
tx-period	EAP retransmission interval
max-req	EAP packet retransmission interval
authenticator mode	Switch authentication mode
Mac Filter	Enables dot1x address filter or not
MacAccessList	Dot1x address filter table
Dot1x-EAPoR	Authentication method used by the switch (EAP relay, EAP local end)
802.1x is enabled on ethernet 1	Indicates whether dot1x is enabled for the port
Authentication Method:	Port authentication method (MAC-based, port-based)
Status	Port authentication status
Port-control	Port authorization status
Supplicant	Authenticator MAC address
Authenticator State Machine	Authenticator state machine status
Backend State Machine	Backend state machine status
Reauthentication State Machine	Re-authentication state machine status

20.4.1.6 debug aaa

Command: debug aaa

no debug aaa

Function: Enables AAA debugging information; the " **no debug aaa"** command disables the AAA debugging information**.**

Command mode: Admin Mode

Parameters: N/A.

Usage Guide: Enabling AAA debugging information allows the check of RADIUS negotiation

process and is helpful in troubleshooting.

Example: Enabling AAA debugging information.

Switch#debug aaa

20.4.1.7 debug dot1x

Command: debug dot1x

no debug dot1x

Function: Enables dot1x debugging information; the " **no debug dot1x"** command disables the dot1x debugging information**.**

Command mode: Admin Mode

Parameters: N/A.

Usage Guide: Enabling dot1x debug information allows the check of dot1x protocol negotiation process and is helpful in troubleshooting.

Example: Enabling dot1x debugging information.

Switch#debug dot1x

20.4.2 802.1x Troubleshooting

It is possible that 802.1x cannot be configured on ports, or 802.1x authentication is set to auto but cannot switch to authenticated state after the user runs 802.1x supplicant software. Here are some possible causes and solutions:

- If 802.1x cannot be enabled for a port, make sure the port is not executing Spanning tree, or MAC binding, or configured as a Trunk port or for port aggregation. To enable the 802.1x authentication, the above functions must be disabled.
- If the switch is configured properly but still cannot pass through authentication, connectivity between the switch and RADIUS server, the switch and 802.1x client should be verified, and the port and VLAN configuration for the switch should be checked, too.
- Check the event log in the RADIUS server for possible causes. In the event log, not only unsuccessful logins are recorded, but prompts for the causes of unsuccessful login. If the event log indicates wrong authenticator password, radius-server key parameter shall be modified; if the event log indicates no such authenticator, the authenticator needs to be added to the RADIUS server; if the event log indicates no such login user, the user login ID and password may be wrong and should be verified and input again.
- Too frequent access to RADIUS data such as run "show aaa" commands may cause the user to be unable to pass through the authentication due to RADIUS data share violation. And the same reason may force users to go offline on re-authentication in the use. As a result, it is recommended to minimize operation to RADIUS data when users are authenticating or re-authenticating.

20.5 WEB MANAGEMENT

Click “Authentication configuration”, to open authentication configuration management list.Users may configure switch 802.1x authentication function.

20.5.1 RADIUS client configuration

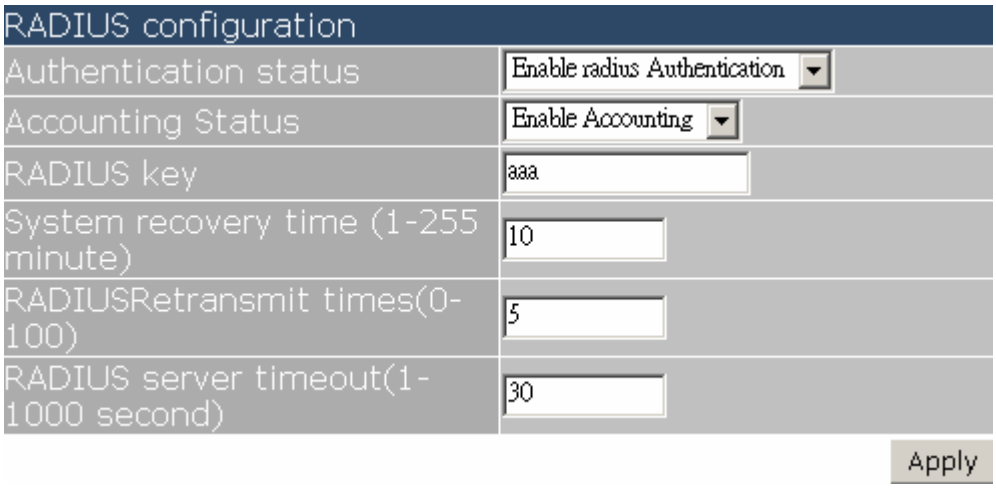
Click “Authentication configuration”, “RADIUS client configuration”, to open Radius client configuration management list Users may the configure switch Radius client.

20.5.1.1 RADIUS global configuration

Click “Authentication configuration”, “RADIUS client configuration”, “RADIUS global configuration” to configure Radius global configuration information:

- Authentication status – Enables, disables switch AAA authentication function. Disable radius Authentication, disable AAA authentication function; Enable radius Authentication, enable
- AAA authentication function. Equivalent to CLI command 20.2.2.1.
- Accounting Status – Enables, disables switch AAA accounting function. Disable Accounting, disable accounting function; Enable Accounting, enable accounting function. Equivalent to CLI command 20.2.2.2.
- RADIUS key – Configures RADIUS server authentication key.（includes authentication and accounting）Equivalent to CLI command 20.2.2.19.
- System recovery time (1-255 minutes) – Configures the recover time after RADIUS server dead. Equivalent to 20.2.2.18.
- RADIUS Retransmit times (0-100) – Configures the number of RADIUS authentication message retransmit times. Equivalent to CLI command 20.2.2.20.
- RADIUS server timeout (1-1000 seconds) – Configures RADIUS server timeout timer. Equivalent to CLI command 20.2.2.20.

Example: Choose Authentication status as Enable radius Authentication, select Accounting Status as Enable Accounting, configure RADIUS key as “aaa”, configure System recovery time as 10 seconds, configure RADIUS Retransmit times as 5 times, configure RADIUS server timeout as 30 seconds, and lastly, click Apply button. The configuration will then be applyied to the switch.

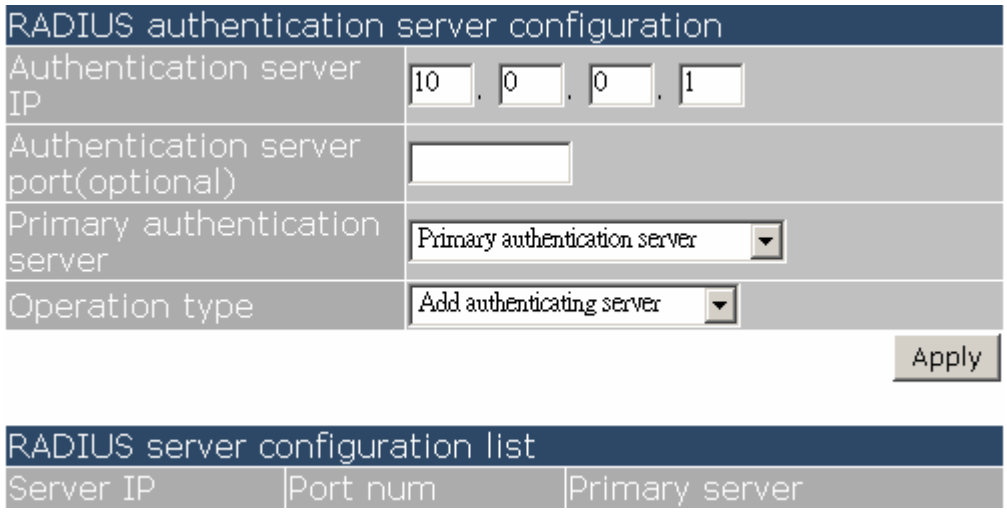


20.5.1.2 RADIUS authentication configuration

Click "Authentication configuration", "RADIUS client configuration", "RADIUS authentication configuration" to configure the RADIUS authentication server IP address and monitor port ID. Equivalent to CLI command 20.2.2.17.

- Authentication server IP – Server IP address. Authentication server port (optional) - Is the server monitor port ID, with range: 0~65535, where "0" means it's not working as an authentication server.
- Primary authentication server – Primary Authentication server, is the primary server; Non-Primary Authentication server, is the non-primary server.
- Operation type – Add authentication server, adds an authentication server; Remove authentication server, remove an authentication server.

Example: Configure Authentication server IP as 10.0.0.1, Authentication server port as default port, select Primary Authentication server, choose Operation type as "Add authentication server", and then click the Apply button, to add this authentication server.

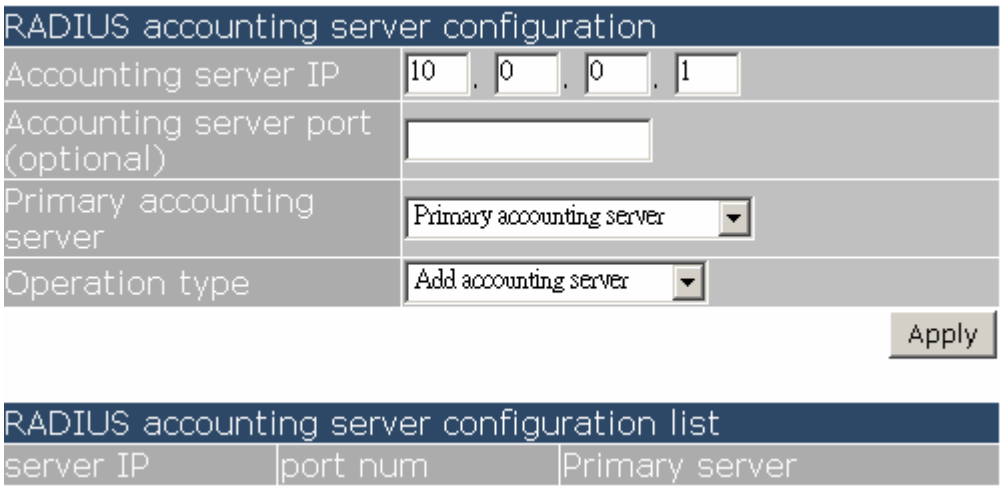


20.5.1.3 RADIUS accounting configuration

Click "Authentication configuration", "RADIUS client configuration", "RADIUS accounting configuration" to configure the RADIUS accounting server's IP address and monitor port ID. Equivalent to CLI command 20.2.2.16.

- Accounting server IP - server IP address.
- Accounting server port(optional) – is the accounting server port ID, with range: 0~65535, where "0" means that it's not work as authentication server.
- Primary accounting server – Primary Accounting server, is the primary server; Non-Primary Accounting server, is the non-primary server.
- Operation type – Add accounting server, adds an accounting server; Remove accounting server, removes an accounting server

Example: Configure Accounting server IP as 10.0.0.1, Accounting server port as default port, choose Primary accounting server, choose Operation type as "Add accounting server" and then click Apply button to add the accounting server.



20.5.2 802.1X configuration

Click "Authentication configuration", "802.1X configuration" to open the 802.1x function configuration management list and configure the switch 802.1x function.

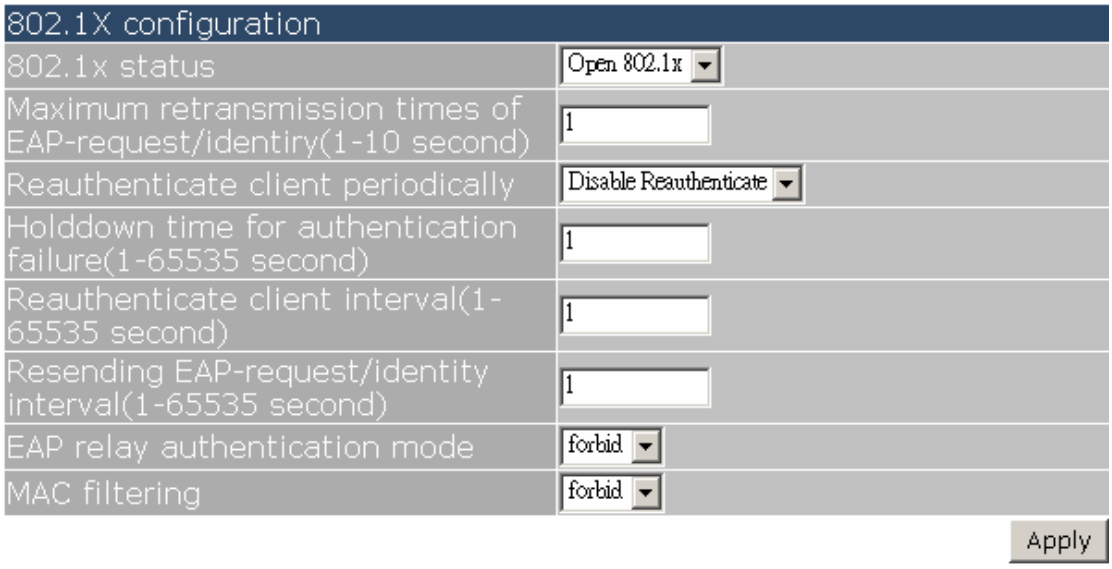
20.5.2.1 802.1X configuration

Click "Authentication configuration", "802.1X configuration", "802.1X configuration" to configure the 802.1x global configurations:

- 802.1x status – Enables, disables the switch 802.1x function. Equivalent to CLI command 20.2.2.5.
- Maximum retransmission times of EAP-request/identity(1-10 second) - Configures sending EAP-request/MD5 frame the maximum times before switch did not receive suppliant response and restart authentication. Equivalent to CLI command 20.2.2.7.
- Re-authenticate client periodically - permit, forbid to make seasonal re-authentication for suppliant. Equivalent to CLI command 20.2.2.12.

- Holddown time for authentication failure(1-65535 second) - Configures suppliant quiet-period status time after authentication failure. Same as CLI command 20.2.2.13.
- Re-authenticate client interval(1-65535 second) - Configures time interval of switch re-authentication client. Equivalent to CLI command 20.2.2.14.
- Resending EAP-request/identity interval(1-65535 second) - Configures time interval of switch retransfer EAP-request/identity frame to suppliant. Equivalent to CLI command 20.2.2.15.
- EAP relay authentication mode - Configures switch to adopt EAP relay method to make authentication; use the "no" command to configure switch to adopt EAP local terminating method to make authentication. Equivalent to CLI command 20.2.2.4.
- MAC filtering – Enables, disables the switch dot1x address filter function. Equivalent to CLI command 20.2.2.6.

Example: Choose 802.1x status as Open 802.1x, Configure Maximum retransmission times of EAP-request/identity as 1, choose Re-authenticate client periodically as Disable Re-authenticate, configure Holddown time for authentication failure as 1, configure Reauthenticate client interval as 1, configure Resending EAP-request/identity interval as 1, choose EAP relay authentication mode as forbid, choose MAC filtering as forbid and then click Apply button to set the configurations.



20.5.2.2 802.1X port authentication configuration

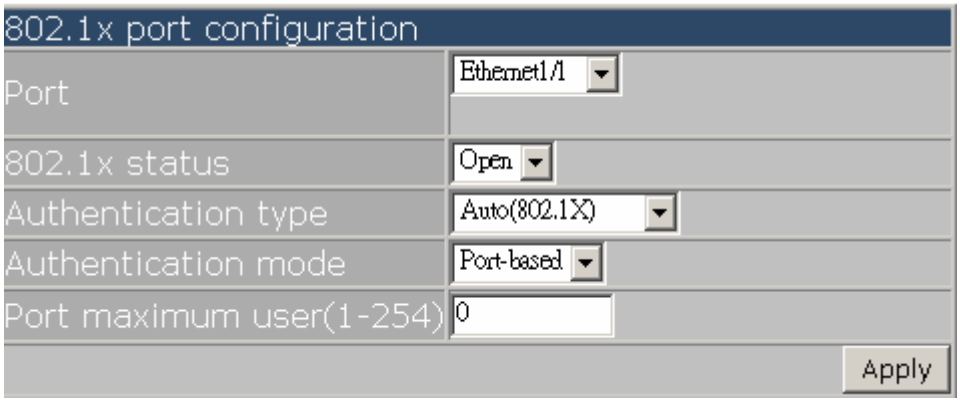
Click "Authentication configuration", "802.1X configuration", "802.1X port authentication configuration" to Configure port 802.1x function

- Port – assigns port
- 802.1x status – port 802.1x status, Open, 802.1x function is open; Close, 802.1x function is close. Same as CLI command 20.2.2.5.
- Authentication type - Configures port 802.1x authentication status. Auto means enable 802.1x authentication. According to switch and suppliant authentication information, to confirm that the port is in authenticated status or unauthenticated status, force-authorized is configured port as authenticated status, allowing unauthenticated data to pass across the port; for force-unauthorized configure port unauthenticated status, switch not provide suppliant authentication service in this port, not permit any port pass across this port. Same as CLI command 20.2.2.9.
- Authentication mode – Configures the access control method for a specific port. Mac-based is access control method which is based on MAC address; port-based access control method

which is based on port. Same as CLI command 20.2.2.10.

- Port maximum user(1-254) - Configures the permission maximum user for specific port. Same as CLI command 20.2.2.8.

Example: Choose Ethernet port1/1, choose 802.1x status as Open, choose Authentication type as auto, choose Authentication mode as port based, configure Port maximum user as 10 and then click the Set button to apply this configuration to switch.

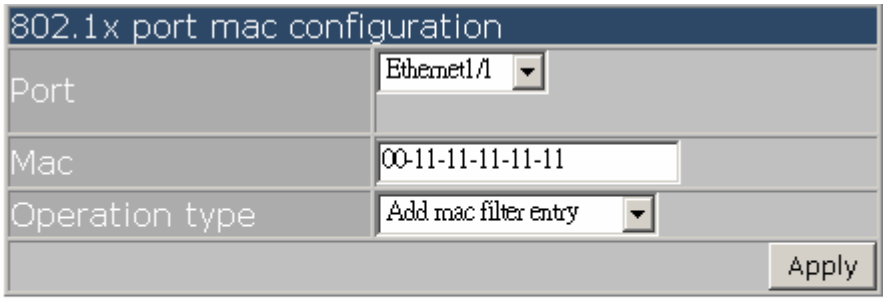


20.5.2.3 802.1X port mac configuration

Click “Authentication configuration”, “802.1X configuration”, “802.1x port mac configuration” to Add a MAC address table to dot1x address filter. Equivalent to CLI command 20.2.2.3.

- Port – If specify port, the added list only suitable for specific port, specify All Ports, the added list suitable for all port.
- Mac – adds MAC address
- Operation type – adds, removes filter MAC

Example: Choose Ethernet port 1/1, configure MAC as 00-11-11-11-11-11, choose Operation type as Add mac filter entry, and then click the Apply button to apply this configuration to switch.



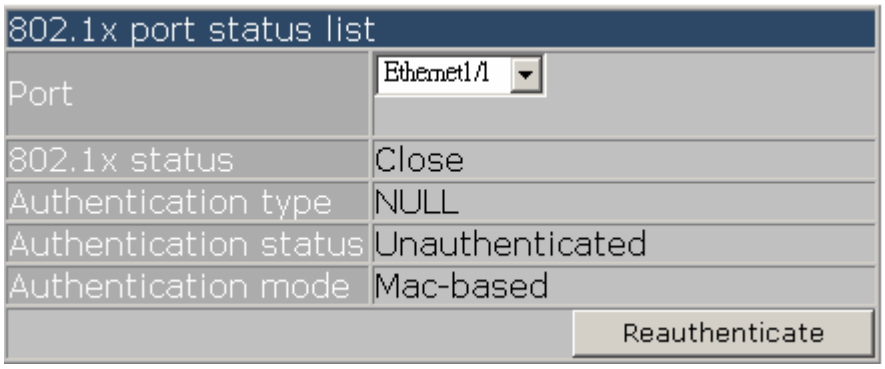
20.5.2.4 802.1X port status list

Click “Authentication configuration”, “802.1X configuration”, “802.1x port status list” to display port 802.1x configuration information, and make re-authentication for the specific port. Same as CLI command 1.2.2.11.

- Port – assign port

- 802.1x status – port 802.1x status
- Authentication type – Authentication type
- Authentication status – Authentication status
- Authentication mode – Authentication mode

Example: Choose Ethernet port 1/1, then Click Reauthenticate button, the user in Ethernet port 1/1 will be force to make re-authentication.



Chapter21 VRRP Configuration

21.1 Introduction to VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault tolerant protocol designed to enhance connection reliability between routes (or L3 Ethernet switches) and external devices. It is developed by the IETF for local area networks (LAN) with multicast/broadcast capability (Ethernet is a typical example) and has wide applications.

All hosts in one LAN generally have a default route configured to specified default gateway, any packet destined to an address outside the native segment will be sent to the default gateway via this default route. These hosts in the LAN can communicate with the external networks. However, if the communication link connecting the router serving as default game and external networks fails, all hosts using that gateway as the default next hop route will be unable to communicate with the external networks.

VRRP emerged to resolve such problem. VRRP runs on multiple routers in a LAN, simulating a "virtual" router (also referred to as a "Standby cluster") with the multiple routes. There is an active router (the "Master") and one or more backup routers (the "Backup") in the Standby cluster. The workload of the virtual router is actually undertaken by the active router, while the Backup routers serve as backups for the active router.

The virtual router has its own "virtual" IP address (can be identical with the IP address of some router in the Standby cluster), and routers in the Standby cluster also have their own IP address. Since VRRP runs on routes or Ethernet Switches only, the Standby cluster is transparent to the hosts with the segment. To them, there exists only the IP address of the Virtual Router instead of the actual IP addresses of the Master and Backup(s). And the default gateway setting of all the hosts uses the IP address of the Virtual Router. Therefore, hosts within the LAN communicate with the other networks via this Virtual Router. But basically, they are communicating with the other networks via the Master. In the case when the Master of the Standby cluster fails, a backup will take over its task and become the Master to serve all the hosts in the LAN, so that uninterrupted communication between LAN hosts and external networks can be achieved.

To sum it up, in a VRRP Standby cluster, there is always a router/Ethernet serving as the active router (Master), while the rest of the Standby cluster servers act as the backup router(s) (Backup, can be multiple) and monitor the activity of Master all the time. Should the Master fail, a new Master will be elected by all the Backups to take over the work and continue serving the hosts within the segment. Since the election and take-over duration is brief and smooth, hosts within the segment can use the Virtual Router as normal and uninterrupted communication can be achieved.

21.1.1 Configuration Task Sequence

1. Create/Remove the Virtual Router (required)
2. Configure VRRP dummy IP and interface (required)
3. Activate/Deactivate Virtual Router (required)
4. Configure VRRP authentication (optional)
5. Configure VRRP sub-parameters (optional)

   1) Configure the preemptive mode for VRRP

2) Configure VRRP priority

3) Configure VRRP Timer intervals

4) Configure VRRP interface monitor

1. Create/Remove the Virtual Router

Command	Explanation
Global Mode	
[no] router vrrp <*vrid*>	Creates/Removes the Virtual Router

2. Configure VRRP Dummy IP Address and Interface

Command	Explanation
VRRP protocol configuration mode	
virtual-ip <*ip*> {master| backup} **no virtual-ip**	Configures VRRP Dummy IP address; **the "no virtual-ip"** command removes the virtual IP address.
interface{IFNAME | Vlan <*ID*>} no interface	Configures VRRP interface, the "no interface" command removes the interface

3. Activate/Deactivate Virtual Router

Command	Explanation
VRRP protocol configuration mode	
enable	Activates the Virtual Router
disable	Deactivates the Virtual Router

4. Configure VRRP Authentication

Command	Explanation
Interface Mode	
ip vrrp authentication mode text **no ip vrrp authentication mode**	Configures the authentication mode for VRRP packets sending on the interface, the **"no ip vrrp authentication mode"** command resets the authentication mode to default value.
ip vrrp authentication string <*string*> **no ip vrrp authentication string**	Configures the simple authentication strings for VRRP packets sending on the interface, the **"no ip vrrp authentication string"** command removes the authentication string.

5. Configure VRRP Sub-parameters

(1) Configure the preemptive mode for VRRP

Command	Explanation
VRRP protocol configuration mode	
preempt-mode {true| false}	Configures the preemptive mode for VRRP

(2) Configure VRRP priority

Command	Explanation
VRRP protocol configuration mode	
Priority < ***priority*** **>**	Configures VRRP priority

(3) Configure VRRP Timer intervals

Command	Explanation
VRRP protocol configuration mode	
advertisement-interval <time>	Configures VRRP timer value (in seconds)

(4) Configure VRRP interface monitor

Command	Explanation
VRRP protocol configuration mode	
circuit-failover {IFNAME | Vlan <*ID*>} **no circuit-failover**	Configures VRRP interface monitor, the **"no circuit-failover"** removes monitor to the interface

21.1.2 VRRP Configuration Commands

21.1.2.1 router vrrp

Commands: router vrrp <*vrid*>

no router vrrp <*vrid*>

Function: Creates/Removes the Virtual Router

Parameters: < *vrid* > is the Virtual Router number ranging from 1 to 255.

Default: Not configured by default.

Command mode: Global Mode

Usage Guide: This command is used to create/remove Virtual Router, which is identified by a unique Virtual Router number. Virtual Router configurations are only available when a Virtual Router is created.

Example: Configuring a Virtual Router with number 10

Switch(config)# router vrrp 10

21.1.2.2 virtual-ip

Commands: virtual-ip <*A.B.C.D*> {master| backup}

no virtual-ip

Function: Configures the VRRP dummy IP address

Parameters: <***A.B.C.D***> is the IP address in decimal format.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a dummy IP address to an existing Standby cluster. The "no virtual-ip" command removes the dummy IP address from the specified Standby cluster. Each Standby cluster can have only one dummy IP, and each dummy IP has two properties: master and backup. When specified as master, the dummy IP address must align to an IP address of an interface in the group, VRRP priority is 255 (no configuration needed), the residing router (or L3 Ethernet switch) interface will be the Master in the Standby cluster. When specified as *backup*, the virtual IP address must not be the same as any interface IP address, and a Master must be elected, and the virtual IP should fall inside the segment of the interface IP addresses.

Example: Setting the backup dummy IP address to 10.1.1.1.

Switch(Config-Router-Vrrp)# virtual-ip 10.1.1.1 backup

21.1.2.3 interface

Commands: interface{IFNAME | Vlan <*ID*>}

no interface

Function: Configures the VRRP interface

Parameters: interface{IFNAME | Vlan <*ID*>} stands for the interface name.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: This command adds a layer 3 interface to an existing Standby cluster. The "**no interface**" command removes the L3 interface from the specified Standby cluster.

Example: Configuring the interface as "interface vlan 1"

Switch(Config-Router-Vrrp)# interface vlan 1

21.1.2.4 enable

Commands: enable

Function: Activates VRRP

Parameters: N/A.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: Activates the appropriate Virtual Router. Only a router (or L3 Ethernet switch) interface started by this enable command is part of Standby cluster. VRRP virtual IP and interface must be configured first before starting Virtual Router.

Example: Activating the Virtual Router of number 10

Switch(config)# router vrrp 10

Switch(Config-Router-Vrrp)# enable

21.1.2.5 disable

Commands: disable

Function: Deactivates VRRP

Parameters: N/A.

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: Deactivates a Virtual Router. VRRP configuration can only be modified when VRRP is deactivated.

Example: Deactivating a Virtual Router numbered as 10

Switch(config)# router vrrp 10

Switch (Config-Router-Vrrp)# disable

21.1.2.6 vrrp authentication mode

Commands: ip vrrp authentication mode text

no ip vrrp authentication mode

Function: Sets the authentication mode for outgoing VRRP packets on the interface, the **"no ip vrrp authentication mode"** command restores the default VRRP authentication mode.

Parameters: "text" set the VRRP authentication mode to Simple String Mode.

Default: Authentication is not set by default.

Command mode: Interface Mode

Usage Guide: This command keeps the VRRP standby cluster from the disturbance of unauthorized members, all switches in the same standby cluster should have the same authentication mode set.

Example: Setting the authentication mode to Simple string mode.

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ip vrrp authentication mode text

21.1.2.7 vrrp authentication string

Commands: ip vrrp authentication string <string>

no ip vrrp authentication string

Function: Sets the authentication string for outgoing VRRP packets on the interface, the **"no ip vrrp authentication string"** command restores the default VRRP authentication string.

Parameters: <*string*> stands for the VRRP authentication string.

Default: There is no authentication string by default.

Command mode: Interface Mode

Usage Guide: This command keeps the VRRP standby cluster from the disturbance of unauthorized members, all switches in the same standby cluster should have the same authentication string if Simple String mode applies.

Example: Setting the authentication string to "public"

Switch(config)#interface vlan 1

Switch(Config-If-Vlan1)# ip vrrp authentication string public

21.1.2.8 preempt

Commands: preempt-mode{true| false}

Function: Configures the preemptive mode for VRRP

Parameters: N/A.

Command mode: VRRP protocol configuration mode

Default: Preemptive mode is set by default

Usage Guide: If a router (or L3 Ethernet switch) requiring high priority needs to preemptively become the active router (or L3 Ethernet switch), the preemptive mode should be enabled.

Example: Setting non-preemptive VRRP mode

Switch(Config-Router-Vrrp)# preempt-mode false

21.1.2.9 priority

Commands: priority <*value*>

no priority

Function: Configures VRRP priority; the **"no priority"** restores the default value 100. Priority is always 255 for IP Owner.

Parameters: < *value*> is the priority value, ranging from 1 to 255.

Default: The priority of all **backup** routers (or L3 Ethernet switch) in a Standby cluster is 100; the Master router (or L3 Ethernet switch) in all Standby cluster is always 255.

Command mode: VRRP protocol configuration mode

Usage Guide: Priority determines the ranking of a router (or L3 Ethernet switch) in a Standby cluster, the higher priority the more likely to become the Master. When a router (or L3 Ethernet switch) is configured as Master dummy IP address, its priority is always 255 and does not allow modification. When 2 or more routers (or L3 Ethernet switch) with the same priority value present in a Standby cluster, the router (or L3 Ethernet switch) with the greatest VLAN interface IP address becomes the Master.

Example: Setting VRRP priority to 150.

Switch(Config-Router-Vrrp)# priority 150

21.1.2.10 advertisement-interval

Commands: advertisement-interval <*adver_interval*>

no advertisement-interval

Function: Sets the vrrp timer values; the **"no advertisement-interval"** command restores the default setting.

Parameters: <***adver_interva***> is the interval for sending VRRP packets in seconds, ranging from 1 to 10.

Default: The default **<*adver_interva*>** is 1second.

Command mode: VRRP protocol configuration mode

Usage Guide: The Master in a VRRP Standby cluster will send VRRP packets to member routers (or L3 Ethernet switch) to announce its properness at a specific interval, this interval is referred to as

adver_interval. If a Backup does not receive the VRRP packets sent by the Master after a certain period (specified by *master_down_interval*), then it assume the Master is no longer operating properly, therefore turns its status to Master.

The user can use this command to adjust the VRRP packet sending interval of the Master. For members in the same Standby cluster, this property should be set to a same value. To Backup, the value of *master_down_interval* is three times that of adver_interval. Extraordinary large traffic or timer setting differences between routers (or L3 Ethernet switches) may result in *master_down_interval* and invoke instant status changes. Such situations can be avoided through extending *adver_interval* interval and setting longer preemptive delay time.

Example: Configuring vrrp Timer value to 3

Switch(Config-Router-Vrrp)# advertisement-interval 3

21.1.2.11 circuit-failover

Commands: circuit-failover <*ifname*> <*value_reduced*>

no circuit-failover

Function: Configures the vrrp monitor interface

Parameters: < *ifname* > is the name for the interface to be monitored

<*value_reduced*> stands for the amount of priority decreased, the default value is 1~253

Default: Not configured by default.

Command mode: VRRP protocol configuration mode

Usage Guide: The interface monitor function is a valuable extension to backup function, which not only enable VRRP to provide failover function on router (or L3 Ethernet switch) fail, but also allow decreasing the priority of a router (or L3 Ethernet switch) to ensure smooth implementation of backup function when status of that network interface is **down**.

When this command is used, if the status of an interface monitored turns from **up** to **down**, then the priority of that very router (or L3 Ethernet switch) in its Standby cluster will decrease, lest Backup cannot changes its status due to lower priority than the Master when the Master fails.

Example: Configuring vrrp monitor interface to vlan 2 and decreasing amount of priority to 10.

Switch(Config-Router-Vrrp)# circuit-failover vlan 2 10

21.2 Typical VRRP Scenario

As shown in the figure below, SWITCHA and SWITCHB are Layer 3 Ethernet Switches in the same group and provide redundancy for each other; SWITCHA is configured as the Master switch.

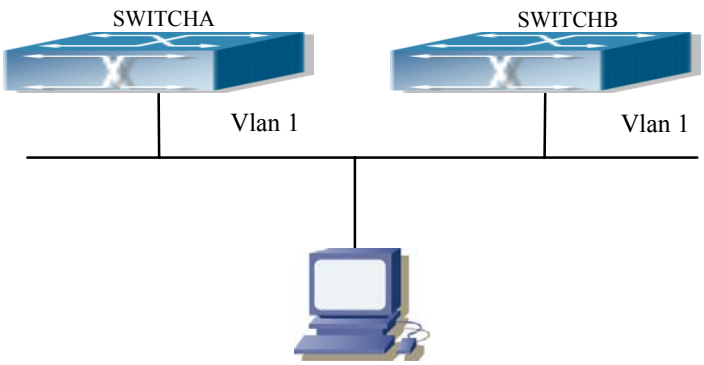


Fig 20-1 VRRP Network Topology

Configuration of SWITCHA:

SwitchA(config)#interface vlan 1

SwitchA (Config-If-Vlan1)# ip address 10.1.1.5 255.255.255.0

SwitchA (Config-If-Vlan1)#exit

SwitchA (config)#router vrrp 1

SwitchA(Config-Router-Vrrp)# virtual-ip 10.1.1.5 master

SwitchA(Config-Router-Vrrp)# interface vlan 1

SwitchA(Config-Router-Vrrp)# enable

Configuration of SWITCHB:

SwitchB(config)#interface vlan 1

SwitchB (Config-if-Vlan1)# ip address 10.1.1.7 255.255.255.0

SwitchB (Config-if-Vlan1)#exit

SwitchB(config)#router vrrp 1

SwitchB (Config-Router-Vrrp)# virtual-ip 10.1.1.5 backup

SwitchB(Config-Router-Vrrp)# interface vlan 1

SwitchB(Config-Router-Vrrp)# enable

21.3 VRRP Troubleshooting Help

21.3.1 Monitor and Debug Commands

21.3.1.1 show vrrp

Commands: show vrrp [<***vrid***>]

Function: Displays status and configuration information for the VRRP standby cluster.

Command mode: All Modes

Example:

Switch# show vrrp

VrId <1>

State is Initialize

Virtual IP is 10.1.20.10 (Not IP owner)

Interface is Vlan2

Priority is 100

Advertisement interval is 1 sec

Preempt mode is TRUE

VrId <10>

State is Initialize

Virtual IP is 10.1.10.1 (IP owner)

Interface is Vlan1

Configured priority is 255, Current priority is 255

Advertisement interval is 1 sec

Preempt mode is TRUE

Circuit failover interface Vlan1, Priority Delta 10, Status UP

Displayed information	Explanation
State	Status
Virtual IP	Dummy IP address
Interface	Interface Name
Priority	Priority
Advertisement interval	Timer interval
Preempt	Preemptive mode
Circuit failover interface	Interface Monitor information

21.3.1.2 debug vrrp

Commands: debug vrrp [**all | event | packet** [**recv| send**]]

no debug vrrp [**all | event | packet** [**recv| send**]]

Function: Displays information for VRRP standby cluster status and packet transmission; the **"no debug vrrp"** command disables the debug information.

Default: Debugging information is disabled by default.

Command mode: Admin Mode

Example:

Switch#debug vrrp

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

VRRP SEND[Hello]: Advertisement sent for vrid=[10], virtual-ip=[10.1.10.1]

21.3.2 VRRP Troubleshooting Help

In configuring and using VRRP protocol, the VRRP protocol may fail to run properly due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ Good condition of the physical connection.
- ✧ All interface and link protocols are in the UP state (use “show interface” command).
- ✧ Ensure VRRP is enabled on the interface.
- ✧ Verify the authentication mode of different routers (or L3 Ethernet switches) in the same standby cluster are the same.
- ✧ Verify the timer time of different routers (or L3 Ethernet switches) in the same standby cluster are the same.
- ✧ Verify the dummy IP address is in the same network segment of the interface’s actual IP address.
- ✧ If VRRP problems persist after the above-mentioned procedures, please run debug gingcommands like “debug vrrp”, and copy the DEBUG information in 3 minutes and send the information to Edge-Core technical service center.

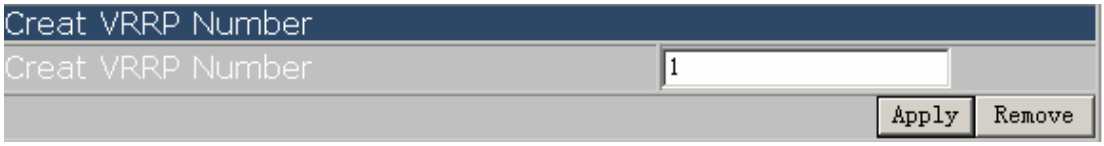
21.4 WEB MANAGEMENT

Click “VRRP control” to enter VRRP control configuration mode to manage VRRP features for the switch.

21.4.1 Create VRRP Number

Click “VRRP control” to enter "Create VRRP Number".

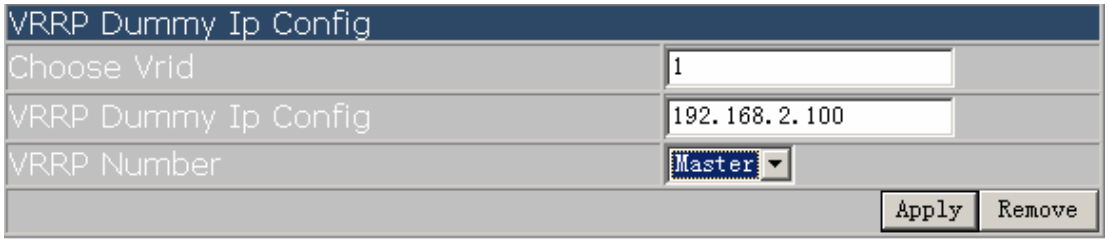
Example: Enter 1 for virtual router number and click Apply to create a virtual router with VRRP number 1. Click Remove to remove Virtual Router 1.



21.4.2 Configure VRRP Dummy IP

Click “VRRP control” to configure VRRP and enter "VRRP Dummy IP Config".

Example: Enter the created Virtual Router number 1, VRRP Dummy IP address 192.168.2.100 and select the VRRP number type to be Master. Click Apply to add the Dummy IP address to Virtual Router number 1 of Master type. Click Remove to remove the Dummy IP address from Virtual Router number 1.

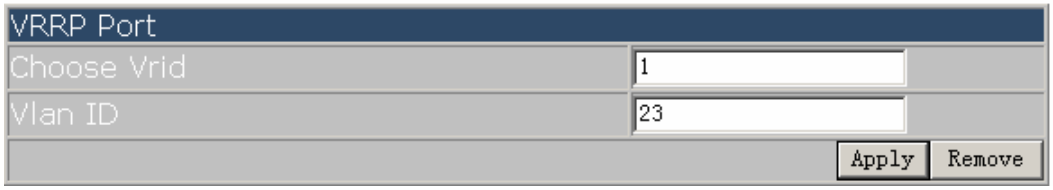


21.4.3 Configure VRRP Port

Click “VRRP control” to configure VRRP and enter "VRRP Port".

Example: Enter created Virtual Router number "1" and VLAN port IP "23". Click Apply to add port 23 to Virtual Router number 1. Click Remove to remove port 23 from Virtual Router number 1.

Notice:Before Interface,please first delete the Virtual IP on the Interface

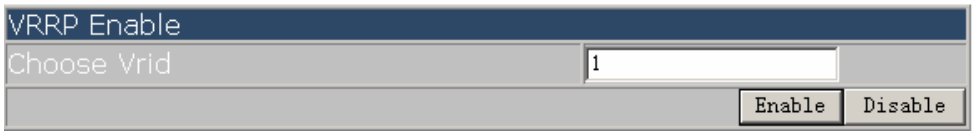


21.4.4 Activate Virtual Router

Click “VRRP control” to configure VRRP and enter "Enable Virtual Router".

Example: Enter the created Virtual Router number "1". Click Enable to activate Virtual Router number 1. Click Disable to deactivate Virtual Router number 1.

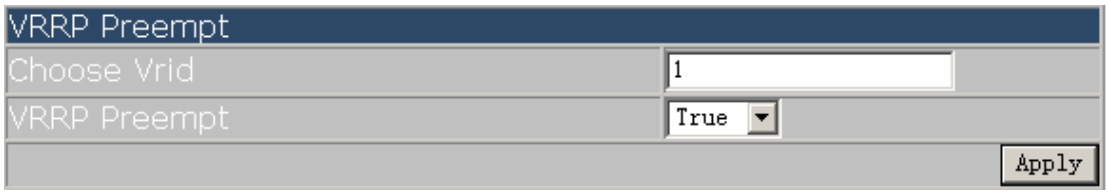
Notice:Before enable VRRP,please finish the setting of Virtual IP and Interface



21.4.5 Configure Preemptive Mode For VRRP

Click “VRRP control” to configure VRRP and enter "VRRP Preempt".

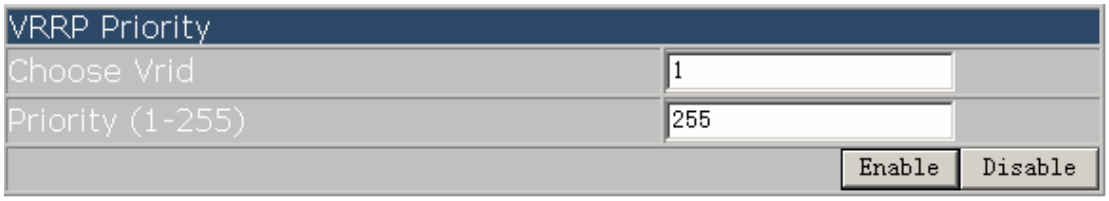
Example: Enter "1" for Virtual Router number and choose TRUE for "VRRP Preempt". Click Apply to configure the preemptive mode for virtual router number 1 to "True".



21.4.6 Configure VRRP priority

Click “VRRP control” to configure VRRP and enter "VRRP Priority".

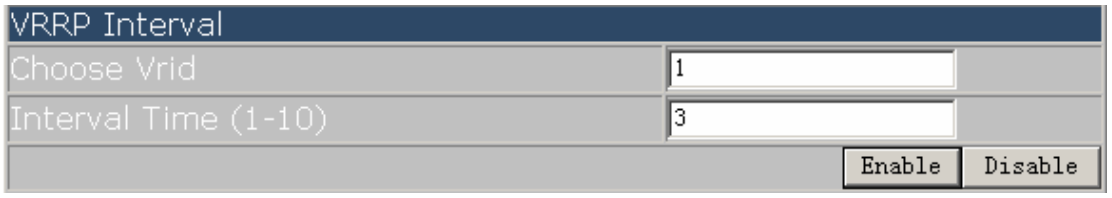
Example: Enter the created Virtual Router number "1" and priority. Click Enable to set the priority of virtual router number 1 to "255". Click Disable to disable the priority of Virtual Router number 1.



21.4.7 Configure VRRP Timer interval

Click “VRRP control” to configure VRRP and enter "VRRP Interval".

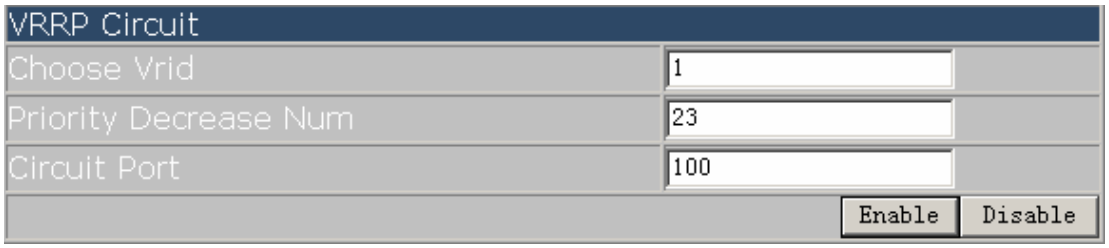
Example: Enter created Virtual Router number "1" and interval "3". Click Enable to set the interval of virtual router number 1 to "3". Click Disable to disable the interval of Virtual Router number 1.



21.4.8 Configure VRRP Interface Monitor

Click “VRRP control” to configure VRRP and enter "VRRP Circuit".

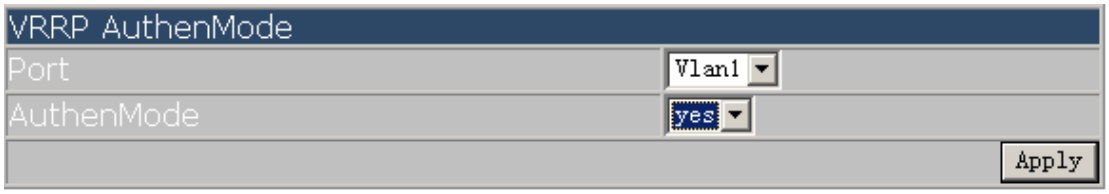
Example: Enter "1" for the created Virtual Router number, 23 for monitor port name and 100 for priority decreasing amount. Click Enable to activate monitor on Virtual Router number 1 port 23. Click Disable to deactivate monitor on Virtual Router number 1 port 23.



21.4.9 Configure Authentication Mode For VRRP

Click “VRRP control” to enter "VRRP AuthenMode" and configure VRRP authentication mode.

Example: Choose created "Vlan1" for Port and "yes" for AuthenMode. Click Apply to finish Port Vlan1 authentication mode configuration.



21.4.10 Configure Authentication String For VRRP

Click “VRRP control” to enter "VRRP AuthenString" and configure VRRP authentication string.

Example: Choose created "Vlan1" for Port and "yes" for AuthenMode and enter an authentication string. Click Apply to finish Port Vlan1 authentication string configuration.